WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Dematerialized Documents Using BlockChain

***Tejaswi Sapala*[1]*, Raj Prakash Karimsetti*[2]*, Meghana Reddy Donadula*[3]*, Dr. A. Vanathi*[4]**

[1,2,3] U.G Student, Department of Computer, Science and Engineering, Aditya Engineering College, Surampalem, A.P., India
[4]M. E., Ph. D., Associate Professor, Head of Department, Science and Engineering, Aditya Engineering College, Surampalem, A.P., India

DOI: https://doi.org/10.55248/gengpi.4.423.35954

ABSTRACT—

Document verification is the first step whenever we enter any organization or institute. In any organization, it is essential to track, verify, and check the person's background who will become a part of the organization. This process is very time-consuming and hectic for both parties involved. Various governments provide cloud-based digital locker services for the citizens storing the public document on a centralized server. But due to its centralized nature, this type of service is weak against information breaches and Denial of Service (DoS) attacks. Also, there are some privacy concerns with such centralized digital locker services as the stored documents may contain users' crucial personal information. This project proposes a blockchain -based digital locker in a decentralized application using Inter Planetary File System Blockchain to securely store personal educational documents with high availability. The proposed solution also verifies documents automatically with ease, confidentiality, access control, data privacy, authenticity, and maintaining the integrity of documents.

Keywords— DoS, IPFS Blockchain,CID.

I. INTRODUCTION

Documents or certificates serve to represent ownership or progress of any type. They exist now, but they do so digitally. A digital proof or certificate is used to acknowledge the ownership of an individual on a certain physical or intellectual entity, just as a digital certificate is used to determine whether a candidate has a degree. The efficiency of this progress has simplified daily life. It has decreased the effort required to transport credentials or papers from one location to another and has decreased the likelihood of fraud or illegal activity. Since physical certificates can be used for a variety of illicit purposes, as the film "Catch me if you can" well demonstrates, switching to digital versions should have resolved the issues.

That is regrettably not the case. Although there were a few minor instances of forging or other illegal activity involving digital certificates at the start of this shift, people eventually prevailed. People came up with inventive ways to uncover security flaws and abuse various security aspects as the technology to create robust certificates to assure authority grew stronger. Due to this, even digital certificates are now susceptible to various forms of forgery and exploitation. People are using hackers (individuals who are proficient in programming but use it for evil) to change things on the internet in order to their advantage.One drawback of the internet is that because of its size, individuals can carry out malicious activities in secret on any part of it, which is encouraging criminal activity, including the use of fake or counterfeit certificates. In order to demonstrate that he has gone to college and earned a degree, a student who has not yetattended college can now have his records uploaded to the system. Similarly Students who have failed a subject or received low grades in it can easily hack the system and modify their grades to make them look good. Despite how difficult the encryptions and safeguards are to breach, hackers continue to find ways around them.

Then there is the issue of willing internal crimes, in which those in charge of the system alter it to portray false values in exchange for financial advantage. The teacher or even the administration, for example, wouldn't know anything about it if the person in charge of entering the student's marks into the system took money from students who had failed and changed the system to indicate that the student had passed in subjects. In local educational institutions, where things like a student's attendance to the entrance and fee payment are being changed, such voluntary internal crimes are becoming more common. Similar to this, more people are getting degrees for job applications without ever having attended college.

A more secure system that can keep records in a very safe manner and aid in preventing such crimes is required in light of the aforementioned detrimental effects of what at first glance appear to be secure digital records systems. Individuals with degrees who lack education should not be allowed to manage social issues because they are detrimental to society. This can only be accomplished if there is a way to safely hold degrees. Similar to how there are many crimes that can be committed in the real estate sector, including crimes involving the management of intellectual property rights and financial assets, these are only a few of the possible offences in the education sector.

Also, managing physical certificates requires a lot of work, so a contemporary method of managing such certificates is crucial. We suggest a Blockchain-based system for storing digital records to remedy this. This approach would use the blockchain to store records securely and guard against manipulation. The core components of blockchain would provide the highest levels of security, as well as aid in spotting any illegal changes and preventing fraud. In order to prevent tampering in the middle, the system would also transfer the necessary certificates securely from one authorised entity to another approved entity. A system like this would increase world security by lowering the amount of crimes and exploitative uses of digital technology incertificatecreation.

II. RELATED WORK

We suggest a blockchain based approach. We use blockchain to both securely store and transfer the records. While blockchain is widely used as a form of payment, we plan to apply the same idea to ensure that records and certificates are securely stored and transferred from one authorised entity to another entity utilising secure transfer techniques. The requisite security and efficiency are successfully delivered by the distinct address system and the impossibility of hacking a blockchain.

Features:

1. **Homepage:**

Faculty and students can utilise this dashboard to view papers like certifications.

For authentication purposes, this page provides both a mobile number and an Aadhar number.

One-time password for Aadhar Number Verification (OTP)

2. **Adminpage:**

Colleges and schools can access Admin.

Admin has access to read, write, and update data.

3. **LoginPage:**

With a login ID and password, Admin can register and log in on the login page. Admin can quickly change the password.

III. FUNCTIONALOVERVIEW

a) RolesandResponsibilities

1) Administrator:Administrators are approved organisations that issue certificates to students; they may be educational or training organisations. These accounts are created on the application by the organisations themselves, and they have access to the profiles of all students listed under their university.

2) Student: The user who requires official certificates from institutions is a student.

b) ApplicationFlow

Viewpoint of the Administrator

i. The institution is granted access to an account.

ii. The institution has students as part of its community.

iii. Using the students' individual identities, the institution administrator can access the students' profiles.

iv. Documents and diplomas are added to the students' profiles.

Student's Point of View

1) The pupil sets up an account.

2) He/she accesses his/her files and looks at the files that organisations have uploaded for him/her.

The crucial point in this situation is that, after the files have been uploaded, nobody will be able to change them. Even if there is a change, it will be obvious who made it because every update and deletion is monitored using the administrator's specific ID. So, this renders the majority ofillegal acts impossible. Even though it appears straightforward, the system offers a blatantly safe method of sharing and displaying confidential information between students and academic institutions.

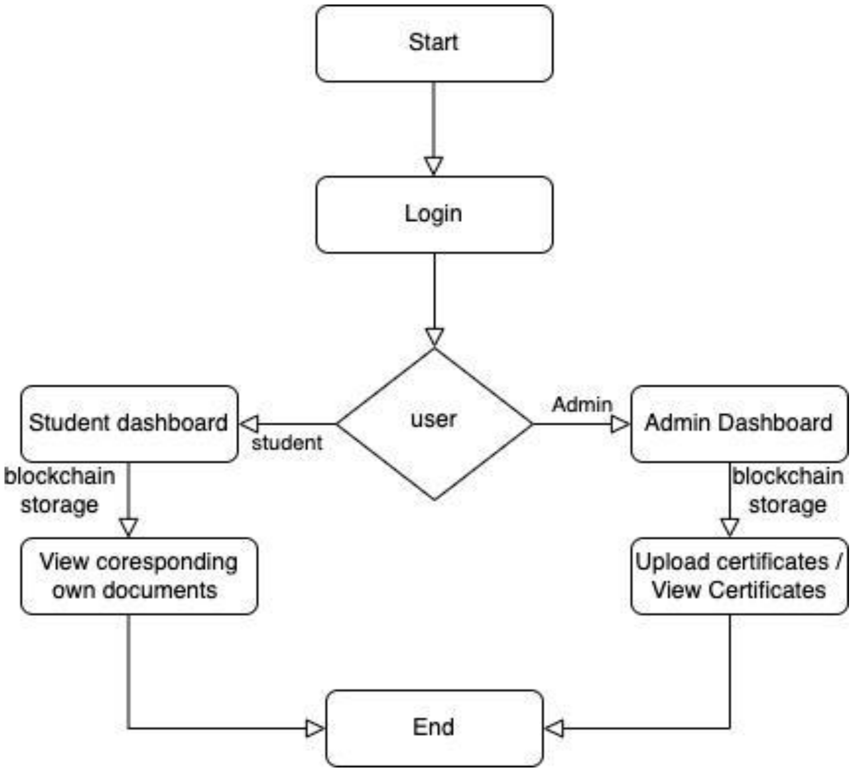

Fig.1.WorkFlow

IV. SYSTEM DESIGN

The following technologies are used for the development of the system.

JavaScript: In this application, JavaScript is used to create the web interfaces, user and admin modules, and to host them on the internet. JavaScript is one of the key technologies that make up the foundation of the world wide web.

Solidity: Smart contracts are created using Solidity, a high-level object-oriented programming language for contracts, using blockchain platforms. It also has several uses when constructing with blockchains and the IPFS network. The blockchain is utilised in this application to link each student's records and keep them on the blockchain. On the IPFS Virtual Machine, Solidity is utilised.

IPFS : InterPlanetary File System is referred to as IPFS. In a distributed peer-to-peer network, this file system is used to distribute and share files and hypermedia. A file is broken up into smaller pieces when it is added to the IPFS, then it is cryptographically encoded and given a special ID, known as a Content Identified (CID)[11], which relates to the file's contents at that particular moment. The distinct ID facilitates access to the file whenever a new request for access to it is received, and this new entity also retains a copy of the file in its cache and acts as a temporary distributor of that particular file.As a result, file data will be preserved chronologically and file tampering will be prevented. When we add a new version of a file, the process is repeated and a new ID is obtained. With this application, files from organisations are handled by IPFS and made available to the students.

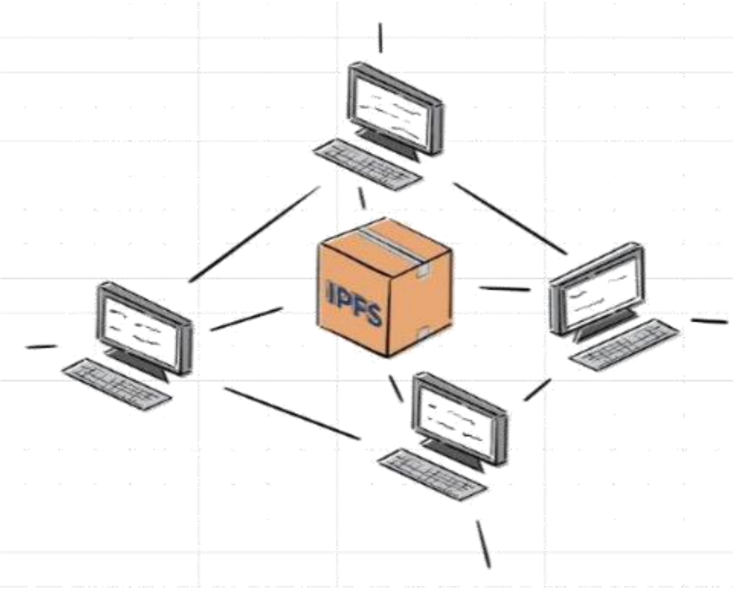

Fig.2.IPFS

V. IMPLEMENTATIONDETAILS

Blockchainstorage

Blockchain storage is a method of storing data in a decentralised network that makes advantage of the free hard drive space of users all over the world. A decentralised infrastructure can address several issues present in a centralised system and is an alternative to centralised cloud storage. Using distributed ledger technology, blockchain (DLT). A decentralised store of data regarding transactions between different parties is what the DLT functions as. Operations are maintained in the ledger as a sequence of blocks and are filled into the DLT in chronological order. A blockchain is made up of interconnected chains of blocks, each of which refers to the block before it. Moreover, 1GB of machine storage space is needed to store and process the data sets.

VisualStudio code

Microsoft created the source-code editor Visual Studio Code, generally known as VS Code, for Windows, Linux, and macOS using the Electron Framework. Debugging support, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git are among the features. The theme, keyboard shortcuts, options, and extensions that offer more functionality can all be changed by users.

Solidity

Programming in a statically typed language called Solidity allows for the creation of smart contracts that work with the IPFS Virtual Machine (EVM). For experienced web developers, Solidity's syntax is similar to ECMAScript; but, unlike ECMAScript, it supports static typing and variable return types. IPFS is a decentralised blockchain platform that creates a peer-to-peer network for safely executing and validating smart contract application code. Participants can do business with one another using smart contracts without the need for a reliable central authority.

We have used a number of frameworks,including Web3.js, jQuery, and CryptoJS, to communicate with the client and blockchain. An HTTP or IPC connection canbe used by Web3.js to communicate with a nearby or distant IPFS node. A JavaScript library called jQuery was created to make HTML DOM tree manipulation and event handling simpler. For SHA256 and AES encryption/decryption calculations, we used cryptoJS. Python-based Flask is a microweb framework. We use it to build the web server that serves the pages as well as to compute hashes and verify signatures. Moreover, it is utilised to send emails utilising the SMTP protocol to users. To send and receive the file from the file server, we use the Dropbox API. HTML and CSS are used in web page design.

VI. CONCLUSION AND FUTURE WORK

We have designed and successfully implemented a system to fulfil the needs of security, immutability, and authenticity in the possession, transfer, and storage of digital documents such as educational degrees, transcripts, or any other credentials and secure their originality and ownership. Blockchain, which serves as a storage system, is its foundation. The blockchain's immutability and peer-to-peer authentication capabilities make it suitable for verifying authenticity, while its behaviour as a ledger informs us of attempts to access it and modify it. Users can upload files and access records using the system's user interface, which uses user authentication from Firebase. The identical documents may also be sent using safe blockchain addresses.This aids in lowering illegal record-transfer practises. Using blockchain, firebase, and solidity, we have created a comprehensive system that ensures data validity, safety, and transparency.

REFERENCES

- A. B. Chavan and K. Rajeswari, "The design and development of decentralized digi locker using blockchain", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), vol. 9, pp. 29-36, 2019.
- J. R. Teja, "Proposing method for Public record maintenance using Block chain", 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI) IEEE, pp. 1-5, February 2020.
- O. S. Saleh, O. Ghazali and M. E. Rana, "Blockchain based framework for educational certificates verification", Studies Planning and Follow up Directorate. Ministry of Higher Education and Scientific Research Baghdad Iraq. School of Computing University Utara Malaysia, 2020
- I. J. Computer Network and Information Security, 2018, 5, 37-44Published Online May 2018 in MECS 2019.05.05
- Muralidharan, S., &Ko, H. (2019). An Inter Planetary File System (IPFS) . 2019 IEEE International Conference on Consumer Electronics (ICCE). doi:10.1109/icce.2019.8662002
- Zyskind G, Nathan O, Pentland AS (2019) Decentralizing privacy: using blockchain to protect personal data, security and privacy workshops (SPW). IEEE
- Abdullah Al Hussain, Md. AkhtaruzzamanEmon, Toufiq AhmedTanna, Rasel Iqbal Emon and Md. Mehedi Hassan Onik,“ASystematic Literature Review of Blockchain Technology Adoption in Bangladesh”, Annals of Emerging Technologies in Computing(AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 1-30, Vol. 6, No. 1, 1st January 2022, Published by International Association of Educators and Researchers (IAER), DOI:10.33166/AETiC.2022.01.001.
- MeelanThondoo, David Rojas-Rueda, Joyeeta Gupta, Daniel H. deVries and Mark J. Nieuwenhuijsen, “Systematic literature review of health impact assessments in low and middle-income countries”, International Journal of Environmental Research and Public Health, vol. 16, no. 11, p. 2018, 2019, Published by Multidisciplinary Digital Publishing Institute, DOI:10.3390/ijerph16112018.
- Amin Jula, Elankovan Sundararajan and ZalindaOthmana, “Cloud computing service composition: A systematic literature review”, Expert Systems with Applications, vol. 41, no. 8, pp. 3809–3824, 2014, ScienceDirect, DOI: 10.1016/j.eswa.2013.12.017.