Research paper on Storing Documents on Blockchain 2021-2022

Soham Toraskar
Department of MCA
Jain (Deemed-to-be University)
Bangalore, India
sohamtoraskar@gmail.com

Dr. A. Rengarajan
Professor, School of CS & IT, Jain
(Deemed-to-be University)
Bangalore
a.rengarajan@jainuniversity.ac.in
8056133788

Abstract— As we know, each year millions of students graduate and the authorities that issue document have seemed to be compromised for the security credentials of student data. Due to a lack of good anti forge techniques, forged documents often get unnoticed. The use of physical copies of documents creates a huge workload as it involves manual verification, paper storage, and manual auditing. My application will use blockchain to store confidential Data like Aadhaar card, PAN card, Vaccine Certificate, etc. and to keep a public record. Documents can never be tempered as blockchain is immutable. There will be primary nodes and secondary nodes. Primary nodes being the official issuers and secondary will be individuals. Ethereum smart contract will be used for most of the blockchain related decisions, Smart contracts will be public as anyone can view the code and validate. it will be using off-chain solution for storage, new storage technology called IPFS (InterPlanetary File System). It is a distributed file system that is unbackable. It stores multiple copies of the data across different machines, for this any individual can give their storage to use and they will be paid with a native cryptocurrency token Strorenium $STRM, which will be listed on crypto exchanges after launch. People who provide more storage will be get a bigger share of STRM for every block. As Ethereum has high gas fees, we will be using Layer 2 solution like Polygon Network.

A. **Keywords: Blockchain, Documents, Cryptocurrency, IPFS, Immutable, Smart Contract.**

II. INTRODUCTION

Promising and providing 100 percent security and authenticity is always very difficult to accomplish. There always remain a loophole or a vulnerability to be addressed. However, making it difficult for hackers and attackers is possible. Every year many individuals forge official documents like Aadhaar card, License etc. In 2019 Aadhaar database info was leaked and sold on the dark web. Our current methods of issuing and storing of documents is not the most secured way. This project focuses on security and immutability of Official documents while keeping everything transparent. By using Web 3 technology which is the future of web, we can solve lot of issues that current methods have. This project utilizes blockchain technologies like Smart Contracts to automate tasks so no middle man is required, we'll be using Ethereum Blockchain. Decentralized Storage solution like IPFS is used for anonymity and security. Blockchain will maintain all the records on the chain i.e., updating documents, issuing documents, etc. All the records and the dates will be publicly available so any individual can validate the authenticity of the documents.

This project aims to enhance issuing and storing Official Documents. This survey paper describes the various functions of this project. The actual design of the various modules and components of this project Official Documents using Blockchain is described in this document, which takes care of various functionalities that project aims to provide a safe and secure way to store official documents on blockchain which can't be manipulated as records are public and changes can be validated. The use of digital documents is increasing around the world due to convenience and high productivity.

However, the digital documents also have some security issues. For example, when a user who has the permission behaves suspicious for their benefit, the digital

document can be easily manipulated. The current way of issuing and verifying certificates and results has been quite bad as evidenced in the number of counterfeit and forged documents cases in the countries like India. Unfortunately, in today's world, fake documents are epidemic. As most of you know there is no difficulty in getting fake documents. As the fake documents precisely look like the originals, it is a difficult task for someone to identify the real and duplicate. Service providers have to go through millions to verify the documents of candidates manually. Every day, thousands of documents are handled by employees and processed, mostly in digital format, others some still on paper which might change in future. document are one of the major headaches for organizations nowadays.

The current methods do not always allow us to detect false information (so we can find multiple workers using the same file at the same time, but different versions). research carried out by prestigious firms such as Coopers & Lybrand, Nolan Norton Institute, EY or Nucleus Research reveals that 90% of a worker's tasks focus on searching and transporting paper documents, and that 30% of employees' time is spent searching for information for their job, or that 7.5% of the documents that are filled ends up getting lost along the way. A generalized chaos which has turned to digitalization to find a solution to all these intrinsic problems. For this reason, more companies been integrating document management solutions that allow them to automate a big of the work processes. These programs can be from recognition of the documents itself (mainly through OCR technologies) to their classification and processing (using artificial intelligence algorithms that understand the content of the file and its relationship with established internal procedures), assures at all times the integrity of the file, information and the security of the data.

III. RELATED WORK

This project Official Documents using Blockchain is implemented for a secure and safe way to issue and store official documents. Documents will be immutable, they can't be forged or duplicated because all the changes in any document will be recorded on the chain and can be validated. For implementing and understanding about this project, I have gone through some survey papers. the digital documents always have some security issues or the other. For example, when a user who has the access to the digital documents can easily manipulate and falsify the document. Using block-chain how we can solve the issues the current document management systems have, unfortunately, in today's world, fake documents are epidemic. As most of you know that in current generation it is very easy to make a fake document. As the fake documents precisely look like the originals, it is cumbersome for the layman to identify the real and duplicate. They explained how blockchain can solve a lot of issues, using Smart Contracts for immutability and automation. No third party is needed for most of the work, how issuing and storing documents process can be increased and also keeping everything transparent. For storing most of them opted for Decentralized storage like InterPlanetary File System(IPFS) in place of regular centralized storage solutions.

a) A similar related survey paper (Pavitra Haveri, 2020) have proposed a framework a solution of using private blockchain which is good for security wise but not good for transparency this proposed framework is does the job for private organization not for government-based documents as public records are important to validate any individual.

b) Similar work (Khalid Salah, Haya Hasan, 2013) proposed a solution to provide originality and authenticity of published and uploaded online free consumption digital content such as music, pictures, movies and books. The solution utilizes a blend of newly emerging technologies that primary includes (InterPlanetary File System) IPFS and blockchain smart contracts. IPFS is used to store digital content with a high integrity and global accessibility to all, and Ethereum smart contract is used to manage, govern, and provide trace-ability and visible history of digital content from its origin to the current version, in a manner that is decentralized and globally accessed with high integrity, availability, resiliency, and transparency.

c) Existing data sharing platforms depend on trusted third party (TTP). Due to the involvement of TTP, such systems lack lot of trust, immutability transparency and security. To overcome these issues, this paper proposed a blockchain-based secure data sharing platform by leveraging the benefits of interplanetary file system (IPFS). A meta data is uploaded to IPFS server by owner and its available for everyone to access..

d) Smart contracts are computer protocols which operate to enforce a physical routine or a set of activities. It consists of contracts that is created for the sole purpose of auditing and enforcing a said protocol within a private network which is immune. It eliminates the need for a human entity or a third party to verify the validity of the activity, it is also Ethereum based solution.

e) Similar work (Ian Zhou, Justin, Lipman, Imran Makhdoom, 2013) authors of this research paper have proposed a blockchain solution based on Ethereum main chain which is not great for small transactions or making changes in the blockchain, the fees of Ethereum main chain is very high compared to other blockchains and also transaction speed is not fast at all.

IV. ANALYSIS

Documents on Blockchain:

This project has been analyzed currently in windows machine, with all its features working flawlessly and without any problems. The processing times are based on internet connectivity, uploading files takes a little time. For the proper working of the Project,the operating system should be connected with the internet. The proposed system uses Metamask wallet, so without private keys no one can access.

Memory Analysis:

Memory analysis is a mechanism of analyzing the systems RAM for the utilized by the proposed system. Whereas, we deduced that the memory utilization for this system is not that high. On the other hand, if we enhance the current model, by adding new features then the RAM utilization will go little bit high.

Hardware Utilization:

For the proposed system, we need no additional hardware devices, just a computer or mobile phone with Metamask and a descent internet connectivity, can be accessed from any part of the world.

Mechanism

Using React Js and Next JS, we have been able to design an amazing website for individual to interreact with the dApp. MetaMask wallet is used for login, it's a simple browser plugin. For this project its connected to Local Ethereum Blockchain made using Ganache. For Storage we are using InterPlanetary File System which is a decentralized storage solution. Truffle is used to code, test and deploy the Smart Contract on Ethereum Blockchain. Web3.js is the bridge that connects Front End to Backend like IPFS and Smart Contracts.
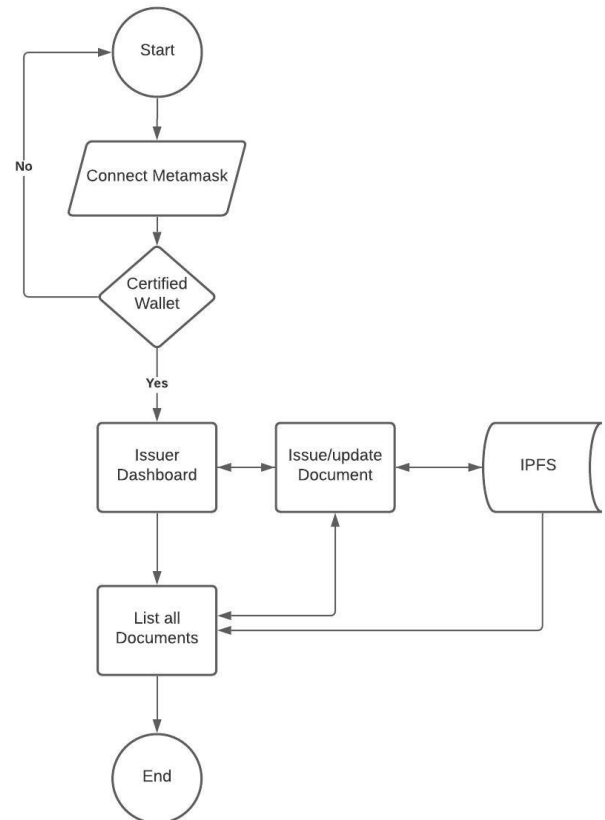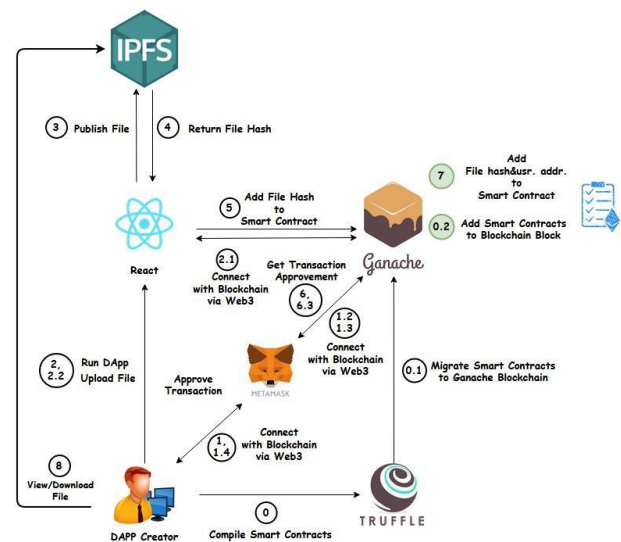
V. INTERPRETATION

Data Flow Diagram of Document Issue Node

Implementation

JavaScript frameworks are used as front end and InterPlanetary File System (IPFS) is used to store documents. The project can be implemented to work with any web browser and it's based on Web3 Technology. React JS and Next JS is used to build the front end as its features are compatible with almost all browsers. Metamask wallet which is a chrome browser extension is used to login and connect to the Ethereum Blockchain. Ganache is used to

create local Ethereum Blockchain, it's used by most Ethereum Developers. Ethereum Smart Contract is used to automate tasks such as issuing documents, updating documents etc. or anything related to blockchain. Truffle is used to write, test and deploy the Smart Contract on Ganache. InterPlanetary File System (IPFS) is used to store and manage Documents, it's a Decentralized Storage solution. The code is implemented and run in any system, which has Ganache, Truffle and Metamask wallet installed. Visual Studio Code text editor is used for all coding. The analysis and the testing of the system is done in a windows environment and no issues and errors have been detected.

VI. Conclusion

To conclude, This project which will be developed using Web 3 technologies like Ethereum blockchain, Smart contracts. This project provides a secure and easier way to issue and store documents. It can be easily implemented and requires a web browser to interact with it. For security we are using Blockchain technology as it's the future, using Polygon(Matic) Blockchain we can use smart contracts which helps eliminate middle man and helps in automating some tasks. Smart Contracts are immutable so no one can hack or change it once its deployed on the Ethereum chain. Duplication, Forging, manipulating etc., is not possible and the records will be public so anyone can validate the document changes. Using IPFS technology we can make it hack proof, IPFS is decentralized storage. Once Document is uploaded on IPFS it can never be deleted or manipulated.

Smart Contracts are immutable once deployed can't be changed. Anyone can validate the document as the records are public.

References

[1] Pavitra Haveri, U.B. Rashmi, D.G. Narayan, K. Nagaratna; K. Shivaraj, "EduBlock: Securing Educational Documents using Blockchain Technology",

[2]Jongbeen Han, Heemin Kim, Yongseok Son "A decentralized document management system using blockchain and secret sharing",

[3] Muqaddas Naz , Fahad A. Al-zahrani , Rabiya Khalid , Nadeem Javaid ,Ali Mustafa Qamar "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System",

[4] Ian Zhou, Imran Makhdoom, Mehran Abolhasan, Justin Lipman "A Blockchain-based Filesharing System for Academic Paper Review",

[5] Khaled Salah, Haya Hasan "IPFS-Blockchain-based Authenticity of Online Publications"