Secure Document transfer with identity and critical information maintenance on Decentralized Web with applications in Education System

Guided by
Prof. Vidya Kurtadikar

Anurag Pardeshi
BE IT B
31540
Email:
Mobile No.:

Gauri Karekar
BE IT C
3154169
karekargauri@gmail.com
+91 99211 65090

Shivansh Nathani
BE IT B
31540
Email:
Mobile No.:

Sujay Mahadik
BE IT B
3154067
mahadik203@gmail.com
+91 90041 33463

Abstract

Database security and easy transfer of documents over the internet have been few of the primary applications of the internet since its inception. But like every other coin, there are some disadvantages of legacy technologies that are being used for the purpose.

We are all aware of the question paper leaks and degree frauds that happen every year in our country. This in turn harms the quality of the Educational System in India. While the Police and Intelligence Departments do their best to prevent such malicious activities, there arises a need for a robust and secure architecture of distribution of question papers, validation of certificates, storing and verifying identities of the candidates.

Technically, blockchain is a decentralized database, spread across many computers with no central control. It is considered to be a technology that could transform governance, businesses, the economy and the functioning of organisations.

We aim at constructing a robust architecture based on decentralized web with the help of technologies like Proof of work and Smart Contracts with IPFS(InterPlanetary File System) as content-addressable file sharing system.

Introduction

A. Lack of Robust Architecture.

Current Centralized Database[1] systems possess a major disadvantage of having a single point failure. Which, stated simply, means that a single server is prone to attacks such as URL Interpretation Attack, Denial-of-Service Attack and many more.

FTP clients use usernames, passwords which are sent over internet as clear texts, allowing attackers to eavesdrop and extract critical information and/or tamper with it.

B. Web 3.0 security

The aforementioned flaws can be easily tackled using Web 3.0. [2] There are a number of advantages that Web 3.0 offers:

- No central point of control
- Complete ownership of data
- Permissionless blockchains

C. Introduction to Blockchain

Blockchain is nothing but a glorified linked list with immutable timestamped entries that are stored in a decentralized peer-to-peer database model.

It all started when Satoshi Nakamoto [3-4] combined established cryptography tools with methods derived from decades of computer science research to enable a public network of participants who don't necessarily trust each other to agree, over and over, that a shared accounting ledger reflects the truth. This makes it virtually impossible for someone to spend the same bitcoin twice, solving a problem that had hindered previous attempts to create digital cash. Also, crucially, it eliminates the need for a central authority to mediate electronic exchange of the currency.

Since then blockchains have found applications not only in cryptocurrencies but also in transforming governance, businesses, the economy and the functioning of organisations.

D. Ethereum Project

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.

These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.

E. Smart Contracts

Smart contracts are self-automated computer programs that can self-execute and self-enforce by using some pre-programmed conditions and run without any possibility of downtime, censorship, fraud or third-party interference.

F. Solidity

Solidity is a contract-oriented, high-level language for implementing smart contracts. It was influenced by C++, Python and JavaScript and is designed to target the Ethereum Virtual Machine (EVM).

Solidity is statically typed, supports inheritance, libraries and complex user-defined types among other features.

Objective and scope of project

The project involves building a decentralized app (DAPP) for applications in Education Systems such as:

- A secure document transfer architecture for distribution of question papers and other critical documents over the internet.
- Consensus-based certificate generation to put a check on degree frauds and maintaining regularities.
- Candidate identity store encrypted using biometric data and/or a private key to facilitate easy authentication, authorisation to exams and other official matters.

The scope of the project is to build an architecture which will be a combination of databases management systems, information security, cryptography and user interface management.

Literature Survey

From the technical point of view, blockchain technology has the following features: decentralization, traceability and immutability.

Decentralization refers to the processes of data verification, storage, maintenance, and transmission on blockchain which are based on a distributed system structure. In this structure, the trust between distributed nodes is built through mathematical methods rather than the centralized organizations.

Traceability means that all transactions on blockchain are arranged in chronological order, and a block is connected with two adjacent blocks by the cryptographic hash function. Therefore, every transaction is trackable by examining the block information linked by hash keys.

There are two reasons that the blockchain technology is **immutable**. On the one hand, all transactions are stored in blocks with one hash key linking from the previous block and one hash key pointing to the next block. Tampering with any transaction would result in different hash values and would thus be detected by all the other nodes running precisely the same validation algorithm.

Potential drawbacks of applying blockchain technology in education[5]

It is undeniable that there are potential drawbacks of applying blockchain technology in education. If an educational blockchain system were put into use in schools, all students' educational data would be integrated into blockchain ledgers. The immutability feature of blockchain technology would act as a double-edged sword. It removes the possibility of modifying educational record for legitimate reasons for some students.

Furthermore, many technical issues or barriers are not addressed for the blockchain to be used in education. For example, the classic Proof of Work consensus mechanism wastes energy and has a poor performance in terms of number of transactions per second (Vukolić 2015), which would cost an extra expense, and hinder its application in schools.

Feasibility Study

The underlying user interface technology or tools used to develop the system will of open source nature mostly open web stack i.e HTML, CSS, JavaScript thus eliminating the cost of buying proprietary software.

The underlying storage API, Inter Planetary File System (IPFS), has been used to create multiple DApps, and the Ethereum Blockchain is one of the most popular Blockchain applications, and is an easy to use framework.

The consensus based certificate generation module will prove to be an effective way to verify and hence to a check on degree frauds.

Software and Hardware requirements

Operating System

The service will work on all three major OS platforms i.e. Windows, Linux Distros and Mac OS. The OS must be modern enough to support the hardware requirements.

Minimum OS Requirements

Windows: Windows 7, Windows 8, Windows 8.1, Windows 10.

Ubuntu: 14.04+

Mac OS: OS X 10.8+

Software

It will mostly be built on JavaScript along with HTML5 and CSS3.

Bootstrap and other web frameworks will be used for the frontend development of the dapp.

The backend code would be done in JavaScript (node.js) and Solidity.

node.js modules used:

ethereumjs-testrpc

web3@0.20.1

solc

Note: Software requirements could increase with the progress of the project. The above are the minimum requirements.

Hardware

System running one of the above OSes. The minimum specifications of the system must include:

2 GB system memory

2 GHz dual processor

1 GB of free space

Internet Access

References

[1] *Nicoleta Magdalena Iacob, Mirela Liliana Moise (December 2015)* Centralized vs Distributed Databases. Case Study, Academic Journal of Economic Studies pp. 119–130 ISSN 2393 - 4913

[2] *Matteo Gianpietro Zago*. Why the Web 3.0 Matters and you should know about it url('https://medium.com/@matteozago/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949')

[3] *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, url('https://bitcoin.org/bitcoin.pdf')

[4] *The Blockchain Review*. Bitcoin, White Paper Made Simple url('https://blockchainreview.io/wp-content/uploads/2018/02/Intrepid-Ventures-Bitcoin-White-Paper-Made-Simple-1.pdf')

[5] *Guang Chen*, *Bing Xu*, *Manli Lu and Nian-Shing Chen*, Exploring blockchain technology and its potential applications for education, Springer Open url('https://slejournal.springeropen.com/track/pdf/10.1186/s40561-017-0050-x')