International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Blockchain based solution for academic certificate management system using smart contract

Smita Chaudhari *, Soham Mohite, Shreya Kumbhakarn, Viren Rathod and Sakshi Khairnar

Department of Information Technology University of Pune, Maharashtra, India.

International Journal of Science and Research Archive, 2023, 08(01), 291–297

Publication history: Received on 30 November 2022; revised on 12 January 2023; accepted on 15 January 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.8.1.0037

Abstract

Educational certificates serve as proof of qualification for their recipients. These certificates are subject to forgery and manipulation. The traditional way to verify the authenticity and integrity of certificates has not shown much efficiency in preventing fraud. Universities and companies need to collect, keep and update an unmanageable number of documents and papers from the applicants, in order to verify the competencies that the applicant claims and to determine forged documents. Another concern is about cyber criminals trying to hack the university's centralized databases to alter the data. Moreover, corrupt officials may be bribed to illegally change a student's academic data without fulfilling the requirements. Blockchain technology has emerged as a new approach to building decentralized reliable systems. It provides an effective and efficient way to protect sensitive data from subsequent change or deletion. Smart contracts decentralize the critical services in the certification process to improve transparency, accuracy, data privacy, and reliability. Unlike the traditional verification methods, the system will be designed in a decentralized way by using blockchain technology. Decentralization enhances the security and robustness features of the system by avoiding single points of failure and removing the need to put trust in any single party.

Keywords: Blockchain; Smart Contract; IPFS; Digital Certificates

1. Introduction

Academic certificates prove that the owners have achieved certain educational accomplishments or fulfilled certain requirements. These documents are used in three distinct processes including issuing, sharing and verification. Reliable verification of academic certificates is of great importance when employing qualified professionals in industry or academia [6]. Universities and companies need to collect, keep and update an unmanageable number of documents and papers from the applicants, in order to verify the competencies that the applicant claims and to determine forged documents. Research shows that more than 30 percent of degrees are falsely claimed. Currently, universities spend more than two million dollars a year to review verification requests [1].

There is further concern about cybercriminals trying to hack the universities databases to alter the data. Moreover, corrupt officials may be bribed to illegally change a student's academic data without fulfilling the requirements. Given the above concerns, it is necessary to use a reliable way of checking the authenticity of these documents so that any manipulation and change in the information can be detected [1]. Blockchain technology has emerged as a new approach to building decentralized reliable systems. It provides an effective and efficient way to protect sensitive data from subsequent change or deletion. Blockchain technology aims at creating a decentralized environment where neither a single entity nor a third party is in control of the transactions and data. The blockchain has also become noteworthy in many other potential applications beyond the digital currency, including creating tamper-proof documents, distributed ownership records, universal medical records, supply chain management, access control, etc [2].

*Corresponding author: Smita Chaudhari

This system is used to collect, store and verify a comprehensive set of academic certificates and provide a reference model for academic evaluation. All the required steps including user registration and identification, issuance process, and verification of certificates are performed on a blockchain using smart contracts on the Hyperledger Fabric platform [4].

2. Literature Survey

In India, the basic structure of a student's studies goes like taking admission in kindergarten, after that changing of school for primary, secondary, and high school studies. Now, after completing high school students, need to get admission into junior college. For graduation, there's also once again changing of college. This is the basic cycle for student's study years. After this, some students continue to pursue higher studies [7].

So, the problem with this cycle is that a student needs to produce all his certificates in each stage for validation. This poses a risk of losing and damaging the certificate. And it is tedious for the validator to authenticate each certificate [5]. With such a huge population in our country, almost every year 26.3 million students graduate. It is very hard to keep track and validate such a huge number of records. Due to this, an unwanted scenario rises i.e., tampering and production of fake or duplicate certificates. There are a lot of hidden agencies in our country who are running this scam behind everyone's back. Technology has moved quite forward until now. Distinguishing between a fake and an original certificate will require a lot of concentration and result in wastage of precious time [8].

For removing this disadvantage, a technology named Blockchain comes into our life as a savior. Because the data in a Blockchain cannot be changed under realistic conditions. Even if data is changed, it just takes a second to let us know about the tampering. In Blockchain a data or a node is validated only when multiple parties approve it. So, the system would be Reliable and Authenticated at any instance of time.

Now, the issue of tampering is solved. The next issue that comes into the picture is time consumption for validation. The system that we will be building will not only validate the certificates but also generate certificates. So it is like killing two birds with one stone. As everything is automated, it takes mere seconds to validate the document [7].

Since everything will be stored digitally, a student doesn't need to worry about losing or damaging the certificate in the process of validation. This proposed system not only removes the loopholes in our current system but also gives us an effective and concrete solution.

3. Related Work

Blockcert[5], is an open standard software built to help applications issue, publish and verify certificates. Blockcert selects a blockchain network like Ethereum or Bitcoin and uses its transactional data to its advantage to store certification records in JSON DL format. Being an open standard, it allows the user to have total control their records. But connecting to a Bitcoin network makes certificate issuing in Blockcert dependent on the Bitcoin prices which vary unstably.

0xcert [1], a similar work like Blockcert, creates a private blockchain network incorporating different types of cryptocurrencies. This leads to two types of charges being levied—for certification and transaction.

CertChain[2] is a certificate management platform which leverages the blockchain technology to provide certificate authentication and prevents counterfeiting of certificates. It uses a public blockchain network with bookkeepers and certificate authorities at each node. Bookkeepers are responsible for accessing the blockchain for recording the certificate operations. The data layer, network layer, extension layer and application layer make up the four-layer architecture which this system uses.

OpenCerts[1] is a platform which uses the Ethereum blockchain to overcome the problem of counterfeit certificates. Using this system educational institutes can create digital copies of the academic certificates that will be issued or have been previously issued. These digitized copies will be published onto the blockchain which provides the certificates with immutability. H. Khandelwal et al. All of the above systems provide an excellent solution for eliminating counterfeit certificates but none of them tackle the issue of identity theft. Also, cryptocurrencies are illegal in most countries, including India.

The hash algorithm namely, SHA-256 is used for sharing certificates as a PDF file other entity. SHA-256 is used for its ability to create a hash from the certificate, but the reverse is not possible. The authenticity of the certificate is preserved by searching the certificate‟s SHA-256 within the index document. If the code is matched, the certificate is authentic. Despite these features to preserve the privacy, ownership, and integrity of certificate, improvements are needed to publicly validate the hash, this is one requirement to allow employers to view the certificate. In addition, the recipient may not be able to authorize a potential employer to verify the certificate using the hash [4].

BCDiploma, EduCTX[9] and UNIC (University of Nicosia) have started their blockchain-based projects to issue and verify diplomas. BCDiploma and EduCTX share the same goal towards a global certification network of higher academic institutions. However, UNIC aims to digitize and decentralize their internal processes having issued their first academic certificates as a proof of concept. Although these approaches are already mature, they either are not meeting the requirements of the UZH or are not easy to integrate into the structure of a university. Therefore, this work shows a prototype that, besides considering these works as starting points, taking into account specific requirements raised from the UZH. For instance, the ease of deployment into their existing IT infrastructure, extending the existing functionality to create diplomas. To guarantee the authenticity of a document, digital signatures can also be used. However, the UZH stated not to apply this solution, mainly because of cost reasons. Also, software exists that can bypass those protections and manipulate the content of a document.

4. Proposed Methodology

Our proposed answer gives ease of figuring out whether or not a record is genuine or now no longer and additionally checking the integrity and originality with the assist of dispensed technology like IPFS and Ethereum smart contracts [1].

- College: College acts as a Certificate issuing authority. This entity may be any company that desires to difficulty a certificate.
- Student: Students will be able to download and view digital documents.
- Company: Company may be the person who can have get entry to concerning originality, authenticity, and integrity of the files with the assist of the virtual signature of the document.

Proposed System involves two processes.

- Publishing

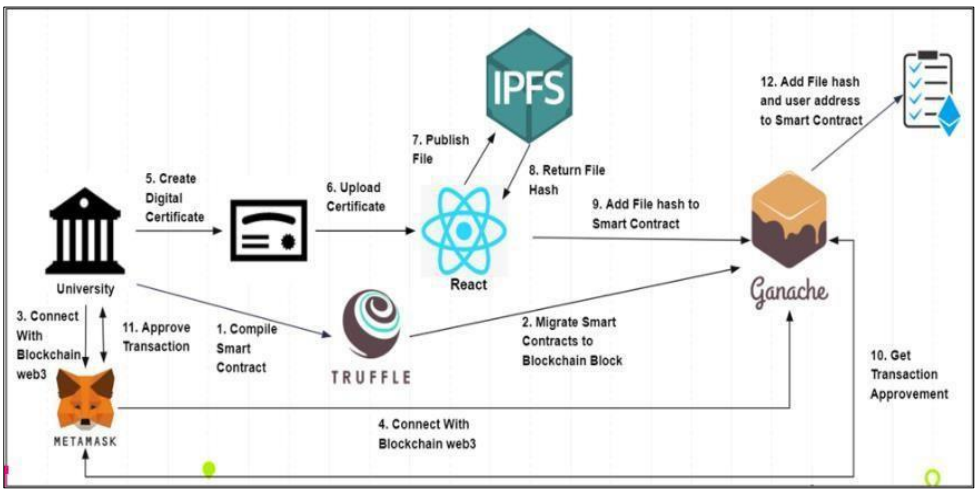

Figure 1 Block Diagram for Publishing Certificate

- Verification

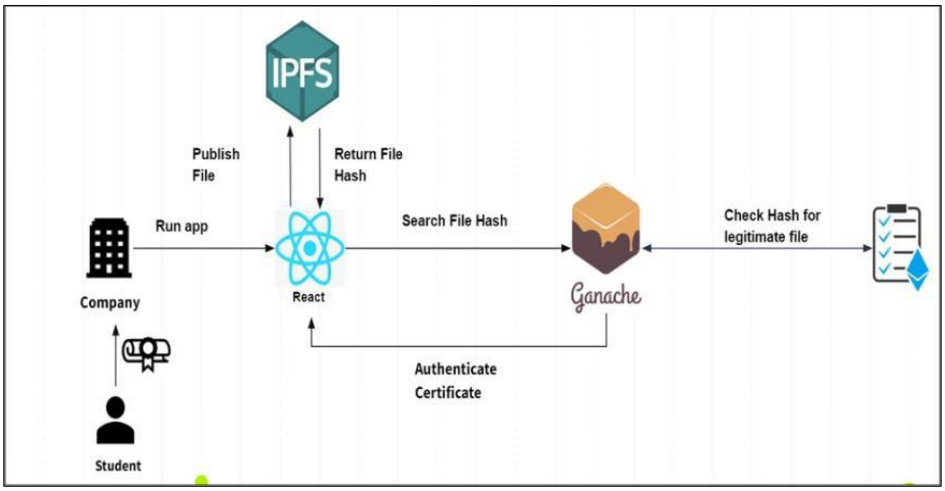

Figure2 Block Diagram for Verification of Certificate

5. System Implementation

5.1. Methodology

As every transaction occurs, it's far recorded as a —block of data. Each block is attached to those earlier than and after it. Transactions are blocked collectively in an irreversible chain.

5.1.1. Ethereum

Ethereum is a decentralized open-supply Blockchain presenting clever settlement functionality. As a blockchain network, Ethereum is a decentralized public ledger for verifying and recording transactions. Ethereum customers pay prices to apply dApps.

The prices are called "gas" due to the fact they range relying on the quantity of computational energy required.

5.1.2. Smart Contract

Smart contracts piece of code that runs on a Blockchain while a person plays a few action. These are truely applications that run while predetermined situations are met.

Smart contracts allow relied on transactions and agreements to be performed amongst disparate, nameless events with out the want for a significant authority.

5.1.3. Solidity

Solidity is an object-orientated programming language for writing clever contracts.
Solidity is noticeably stimulated through C++, Python and JavaScript and has been designed to goal the Ethereum Virtual Machine (EVM).

5.1.4. Metamask

Metamask: MetaMask is an extension for having access to Ethereum enabled allotted programs or ||Dapps|| to your browser. It lets in customers to get entry to their Ethereum pockets via a browser extension.

5.1.5. Ganache

Ganache is used for trying out Solidity contracts on a non-public Ethereum Blockchain.

It is used for permitting you to develop, deploy, and check your dApps in a secure and deterministic environment.

5.1.6. Truffle

Truffle affords clean compilation, linking, deployment, and binary control of clever contracts written in solidity language.

It is trying out framework and asset pipeline for blockchains the use of the Ethereum Virtual Machine (EVM), aiming to make lifestyles as a developer easier.

5.1.7. Node JS

Node JS is used to put in writing backends and is answerable for serving frontend pages, belongings and dealing with consumer authentication the use of JWT (Json Web Token).

It's used for conventional net web sites and back-stop API services, however turned into designed with real-time, push-primarily based totally architectures in mind.

- Implementation

Figure 3 Upload PDF

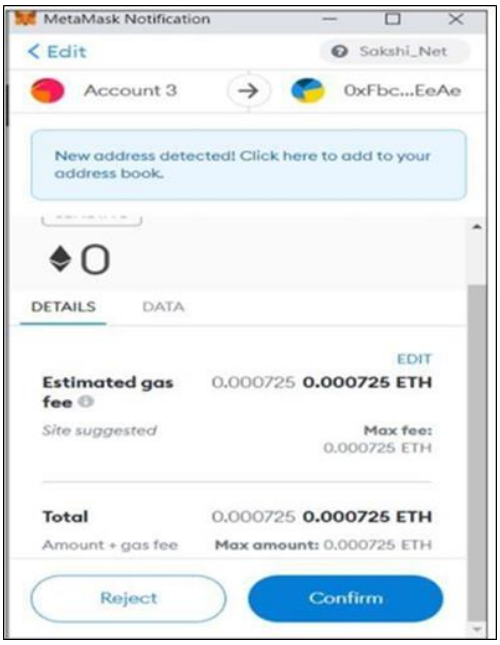

Figure 4 Ethereum Spend for Transaction

Figure 5 Hash calculation of Uploaded File

Figure 6 Hash value of uploaded PDF with IPFS

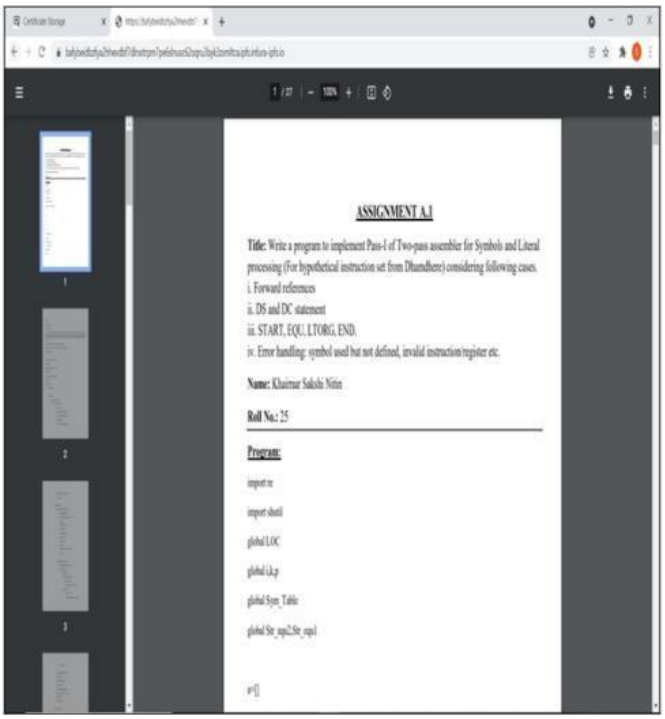

Figure 7 Retrieve PDF using Hash value

6. Conclusion

Automating the issuance and verification of tamper-proof certificates ensures that companies hire qualified people. This approach takes advantage of distributed processing to make it virtually impossible to modify or tamper with sensitive information. This property reduces the likelihood of fraudulent acts and can offer a high degree of privacy through smart contracts.

References

[1] H. Khandelwal, K. Mittal, S. Agrawal, and H. Jain,—Certificate verification system using blockchain‖ in Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies. Springer, 2020

[2] Ahmed Badr, Laura Rafferty, Qusay H. Mahmoud, Khalid Elgazzar, Patrick C. K. Hung, —A Permissioned Blockchain-Based System for Verification of Academic Records IEEE access, 2019.

[3] Alireza Movahedian, Arash Deldari, —Blockchain-based solution For Academic Certificates Management Using Smart Contracts. 10th International Conference on Computer and Knowledge Engineering,October 29-30, 2020

[4] Grech and A. F. Camilleri, —Blockchain in education, Publications Office of the European Union, 132 S. - JRC Science for Policy Report 2017

[5] Eman- Yasser Daraghmi, Yousef- awwad Daraghmi, And Shyan-ming Yuan, —MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management , IEEE access vol. 7, 2019

[6] Emmanuel Nyaletey,Reza M. Parizi, —BlockIPFS - Blockchain-enabled Interplanetary File System for Forensic and Trusted Data Traceability‖ ,IEEE July 2019

[7] E.-Y. Daraghmi,Y.-A. Daraghmi, and S.-M. Yuan,—Unichain: A design of blockchain-based system for electronic academic records access and permissions management, Applied Sciences, vol. 9, no. 22, p. 4966,2019.

[8] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere, and B. Stiller, —The proposal of a blockchain-based architecture for transparent certificate handling, in International Conference on Business Information Systems. Springer, 2018

[9] M. Turkanovic, —Eductx: A blockchain-based higher education credit platform, IEEE access, vol. 6, pp.5112–5127, 2018