International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Decentralized Application for Digital Certification

Aravind G, M S Sowmya, Varun K
Department of Information Science, Jain University,
Jakkasandra, Karnataka, India

ABSTRACT

The rise of fraudulent cases seems to be a nuisance to an organization as they're an investment of money. Various resources also gives the impression to be on someone else, who has false claims. The verification process of these organizations are long and tedious process where the organization would have lost its time and resource on. Blockchain technology was introduced fairly recently in literature, which is the underlying technology behind the very popular cryptocurrency Bitcoin. The blockchain is a decentralized approach, it is secured by design network which was to overcome double spending problem by a central server. The concept of central servers is eradicated in this architecture, where the data is distributed across geographically on separate ledgers. Blockchain applications have diversified as MIT Media Labs introduced Blockcerts for certification of academic records. Ethereum is a platform for developing these decentralized applications using Blockchain ledgers. Ethereum uses a concept called Merkle trees which is the concept used for verification through hashing. As per the working in the literature; this application would make verification of academic documents simple and quick with the usage of Blockchain clients such as Ethereum and an IPFS hash. In this paper we propose a system that provides a solution that addresses the above mentioned issues.

Keywords: *Blockchain, Ethereum, Certification, Decentralized*

I. INTRODUCTION

Blockchain technology provides immutable transactions, that is the details of the transaction cannot be altered. This opens up numerous opportunities not only for payment but also for certification.The project comprises of an application which would provide information about the certification of student's educational qualification which is digitally signed by the university/Education Board and verify the certificate that is created using blockchain technology. This is also applied to POA or POI documents like E-Aadhaar but with a different use of technology.

II. BACKGROUND WORK

Despite blockchain being in its initial stages, a lot of applications and services are being rapidly developed. Services such as transfer of money, proof of consistency, proof of ownership, smart contracts and various other concepts. The blockchain is even will be used for voting in the distant future. But what concerns us the most is its robustness and immutability. Upon looking up these concepts enabled us to envision the project which can be used in any institution and alleviate many difficult processes.

Blockchain is the technology used in the digital cryptocurrency known as Bitcoins. This technology was developed by a group known as Satoshi Nakamoto to solve the double spending problem which was the problem of duplication/falsification. This paved way for a transaction without a trusted authority or a central server.

Web 3.0, a term coined for the change in the protocol of the Internet. At the moment, the majority of the internet works on a centralized network where there is always a central server look after functions of the network. Since the introduction of bitcoins, the technology behind it is being applied to the web as well. Decentralization is the key word here, which tells how Web 3.0 is totally a different path from the old Web 2.0. The protocols behind the new Web are in contrast with the old version, which means many applications are to be built from a scratch.

Upon looking up the subject digital certification, one of most frequently occurring paper would be the MIT digital certificate paper. This provided the foundation for the application which we wanted to develop. This paper redirected to the new initiative which was undertaken by MIT known as Blockcerts. This initiative was led by MIT Media Labs and Learning Machine. Learning Machine is a company which is solely dedicated to decentralizing records which along with the partnership with MIT Media Labs co-created Blockcerts. Blockcerts is an open source standard for digital certification. It is aligned with the following Decentralization and Data Signature standards.

IMS Open Badges

- W3C Verifiable Claims
- W3C Linked Data Signatures
- W3C / Rebooting Web of Trust Decentralized

Identifiers
With these standards, Blockcerts assert that a viable application can be created on a decentralized system.

The Maltese government has partnered with Learning Machine to provide digital academic certification allowing its people to store their academic qualifications and other records for free. Holberton School, which was the first institution to issue digital certificates to students. Holberton School has partnered up with Bitproof, a company which is focused on producing digital certificates. This reported enabled employers to find at least 86% of the employee who lied on their resume. Bitproof also now provides developer tools to create certificates and also enable to develop blockchain applications as well.Sapien's Project was a digital certification project which focused on something little different. It focused on scalability of blockchain technology. They state that Lisk Sidechain would be able to provide SDK's for local computation which is less cost effective and scalable with high computation processes.

Proof of Existence, a blockchain based website which is used to prove the existence of a document. It was noted that some amount of money had to be paid as miner fee. Another observation was that word processing documents were not advisable. This is because word documents possessed metadata, the cryptographic digest generated is solely based on the document's content. So, the metadata of the document does not enable the blockchain to verify the existence of the document at the timestamp. This proves how exact the document must be for the blockchain to verify it. PDF and other unalterable format would be better for this usage.

III. PROBLEM DEFINITION

Certificates are signals of achievement or membership and some are more important than others. University degrees (a particular type of certificate) can help candidate get the job he want, or prevent him from getting it if he doesn't have the right certificate. The current system is very slow and takes lots of time to get the verification done. Whereas digital certificates can be instantly verified. The design of the certification system must be done with utmost thought and precision as it will be used many professional organiza

Many aspirants like to pursue higher education at countries which specialize in a particular domain. Application to such universities requires document verification which is done by contacting the respective schools and colleges to provide confirmation about the applicant's qualification.

Similarly, in business companies perform background and educational verification of their employees. The reason behind such verification is that across the globe there are numerous fraudulent cases. Employee and students are found to have duped or lied in their resume about the certifications. This confirmation is done only done in the later stages of the verification process and would have given enough time for the fraudulent to have taken advantage over the company or university.

Time is wasted upon performing such tasks. On paper nothing seems to be believable unless confirmed by the board or institution. There are many such cases even in India. For instance the Dr. BR Ambedkar University in Agra is alleged to have handed out thousands of fake degrees. Over 100s of fake degrees have been to relatives of the employees of the university. This wasn't confirmed until mid-2015.

A survey conducted by CareerBuilder showed that over 58% of the employee lie in their resume. Only 7% of the employers are willing to overlook resume lie for the candidate. Over 50% employers check for educational qualification suggested the HireRight article.

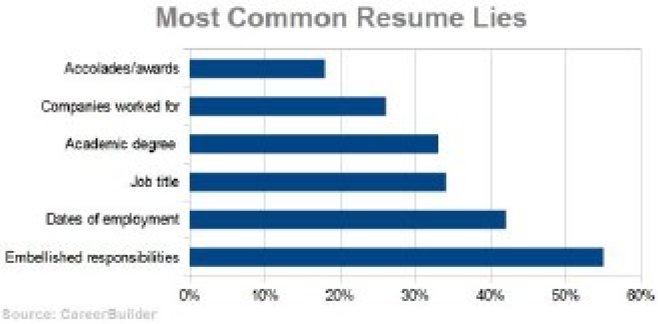


Fig 1.1: Statistics of lies in Resume.

From Fig.1.1, we can notice that over 30% of the resume lie are academic degree. To prevent such fraudulent cases and also provide an ease of presentation of information to the respective organization is one of the reasons behind such a project.

IV. IMPLEMENTATION

A. ARCHITECTURE

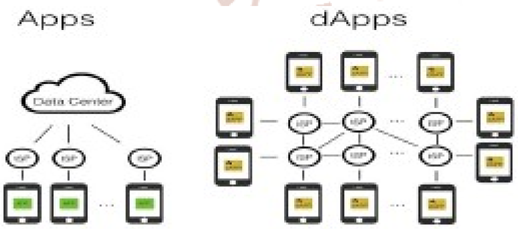


Fig 1.2:Difference between an app and a Dapp

The proposed system which is discussed is not a centralised web application but a decentralized one.The figure above shows the difference between a centralised application and a decentralised one. DApps are applications that utilise the concept of Blockchain which was discussed earlier. ISPs do not locate in to a single server which is the core of the network. In this type of application there is no central server, the data is distributed across various ledgers and the network must work through all the required ledgers that lead to the final one. Below we discuss on how the Dapp's architecture is constructed.

The Fig 1.3 describes the system architecture of the proposed system. in this architecture the client uses a Blockchain client interface for Ethereum orany lightweight client such as Metamask in the front end of the web application. The front end also comprises of web application which is run on Node JS as the server environment. The intermediate section utilizes the web3.js library and its APIs. These APIs are used to interact with the smart contracts which are written for the backend of the application. Finally the backend consists of the blockchain which is embedded with a smart contract. These contracts are invoked when a certain event occurs or is called by the middleware APIs. After invoking these contracts a certain computation is performed on the blockchain. Either a data is posted into the blockchain or retrieved from it. In this case the hash is received and verified.

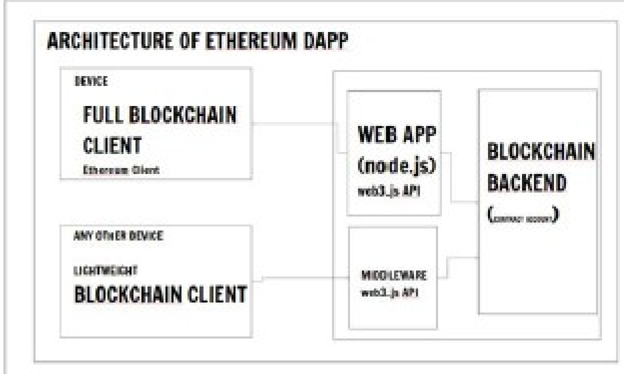


Fig.1.3 Architecture of proposed system

B. TEST NETWORK

There are several networks present on Ethereum. The main network is the network where real transactions of ethers take place. In a development environment, paying actual money is not feasible because of the reiterations of the transactions. The other three development test networks are Rinkeby, Kovan and Ropsten. One of these networks had to be chosen for the development test network. Ropsten was chosen because it provided an environment close to the main network with the Proof of Work consensus algorithm.

C. SOLIDITY SMART CONTRACTS

Initially before constructing the server framework of the application, we first design the interactions of the code with the blockchain. Solidity is sa statically typed language, meaning type checking is done at compile time over run time. In the development of this application we require it to perform the necessary interactions with blockchain. These interactions include setting maximum gas limits, setting the amount of ether for the transaction, input the data such as the hash into the blockchain. The coding of the smart contract in the Remix IDE provided by Ethereum. This allows the contract to be deployed onto the blockchain using the Web3.js injection and Metamask.

D. NODEJS

With basic foundation to the HTML and CSS of the front end of the application,that is the creation of forms and input fields, the server side of the application was coded in NodeJs. Providing multiple pages of HTML and redirecting/rendering the templates was the task of this framework. Node Js is used to control the flow of the application, meaning upon an event, to which template must the server redirect to and also is used for error validation.

E. WEB3.JS

web3.js is a Javascript library which is used to interact with the smart contract which is deployed in the blockchain. web3.js is not only used to help create instances of the smart contract in the application but also to detect the presence of a valid account in the metasmask plugin. This helped in validating if the user is using Metamask and has an account on it or not. It is used to retrieve the transaction id or the hash of the transaction. web3.js is included after the preparation of the basic skeleton of the application.

F. METAMASK

This plugin provides a convenient way of handling the transactions that happens on web browsers. It allows the user to load the private key of their blockchain client account(Ethereum account) into the plugin. Despite sounding susceptible, Metamask provides a very secure method of initiating a transaction. As present in the figure down below, the interface provided is much simple and interactive. it also provides the usage of multiple accounts. All the parameters of the transaction are modifiable accordingly as sometimes the gas units need to be increased to make the transaction a success. Besides that it allows web3.js to detect the public key (Ethereum address) of the user.

G. METAMASK

To provide a module where people can verify the certificates we wanted it to be separate from the certificate creator as the end users are different. The complexity of this module was not as demanding as the certificate creator. This gave rise to the usage of a simple yet powerful Python web framework in the form of flask. The other reason for choosing of flask was to test out some IPFS modules on Python as well. A basic front end with a form which has two inputs and a submit button was created and redirection to successful verification and failure pages were made, providing the flow to the module.

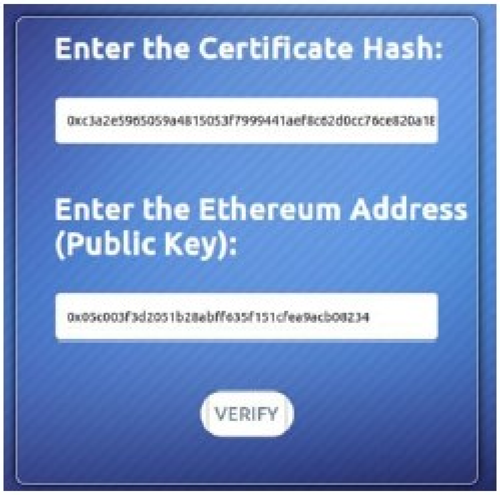
H. FLASK

To provide a module where people can verify the certificates we wanted it to be separate from the certificate creator as the end users are different. The complexity of this module was not as demanding as the certificate creator. This gave rise to the usage of a simple yet powerful Python web framework in the form of flask. The other reason for choosing of flask was to test out some IPFS modules on Python as well. A basic front end with a form which has two inputs and a submit button was created and redirection to successful verification and failure pages were made, providing the flow to the module.

I. ETHERSCAN API

Etherscan provide APIs to query some of the transactional data on the blockchain. Etherscan also provide APIs for test networks such as Ropsten as well. Using Postman API along with API key provided, the queries were made. This enabled to return a JSON file which comprises of most of the transaction data of the address. Despite these API's being in beta(providing upto 1000 transactions only), the data provide was enough for testing. Retrieval of transaction hash of the address was made possible by parsing through the JSON file and can be compared with the entered hash by the user

V. RESULTS



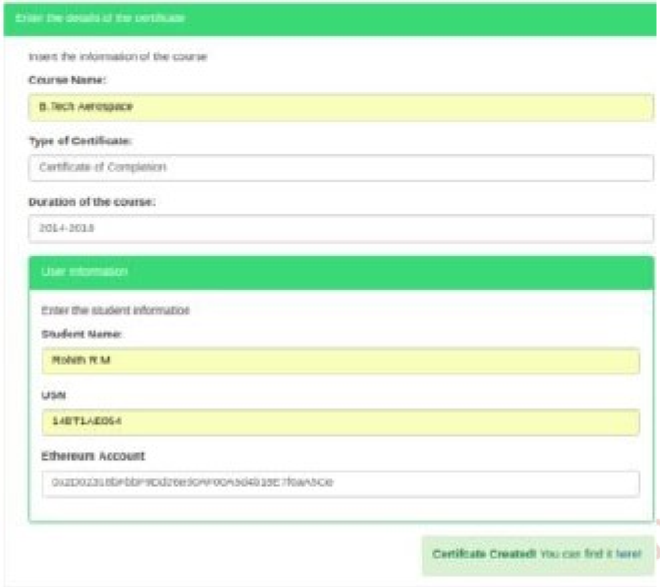
Enter the Certificate Hash:

0xc3a2e5965059a4815053f7999441aef8c62d0cc76ce820a1E

Enter the Ethereum Address (Public Key):

0x05c003f3d2051b28abff635f151cfea9acb08234

Fig 1.4: Certificate verifier form



Enter the details of the certificate

Insert the information of the course

Course Name:

B.Tech Aerospace

Type of Certificate:

Certificate of Completion

Duration of the course:

2014-2018

User information

Enter the student information

Student Name:

Rohith R M

USN

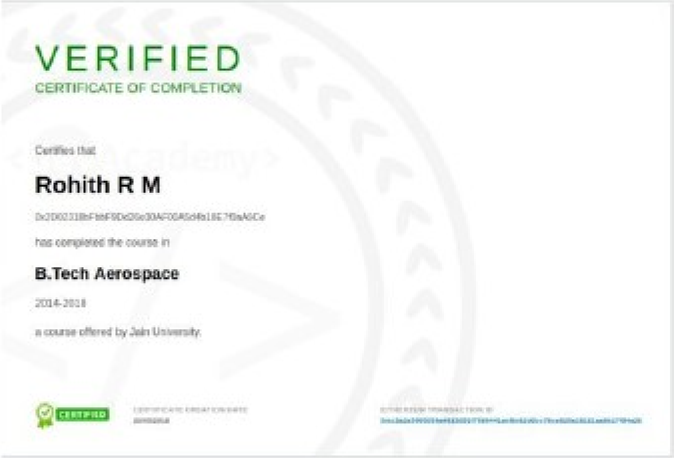
14BTLAE064

Ethereum Account

0x2D02318bFbbF9Dd26e30AF00A5d4b18E7f0aA5Ce

Certificate Created! You can find it here!

Fig 1.5: Certificate creation form



VERIFIED

CERTIFICATE OF COMPLETION

Certifies that

Rohith R M

0x2D02318bF6bF9Dd26e30AF00A5d4b18E7f0aA5Ce

has completed the course in

B.Tech Aerospace

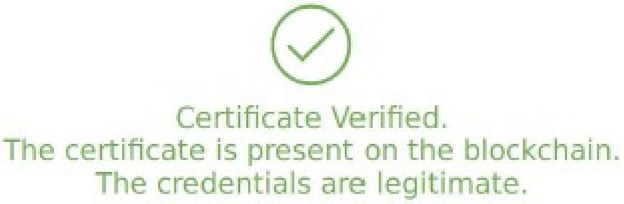
2014-2018

a course offered by Jain University.

CERTIFICATE CREATION DATE
[illegible]

ETHEREUM TRANSACTION ID
[illegible]

Fig 1.5: Certificate with transaction hash



Certificate Verified.
The certificate is present on the blockchain.
The credentials are legitimate.

Fig 1.6:Verified status.

VI. CONCLUSIONS

Blockchain is an innovation that plainly has applications in the realm of learning at the individual, institutional, gathering, national and worldwide levels. It is significant in a wide range of settings: schools, universities, colleges, MOOCs, CPD, corporate, apprenticeships, and information bases. Rather than the old progressive structures, the innovation turns into the concentration, with trust relocating towards the innovation, not the organizations.

It should likewise be perceived that blockchain isn't without its issues. There are data regulation issues, and a cloud has been made over the innovation by the way that one of the trades in the Bitcoin framework – which depends on blockchain – saw $500 million vanish. What's more, last however surely not slightest, after extensive trouble, US experts could shut down the scandalous "Silk Road" sedate managing trade, which was likewise blockchain based.

However the greatest impediment to blockchain's more broad spread utilization is cultural. Education is a crawler in terms of adopting new technologies into its domain. Regardless of its undeniable points of interest, the education field is probably going to be slow in executing this innovation, as the majority of the subsidizing and culture is based on the individual organization.

In terms of technology, this application would be enhanced with the usage of IPFS hashes. IPFS hashes are the hashes generated from the content of the document. The issue limiting the application of IPFS hashes to this project would be that during the implementation of IPFS hash in our system, a different hash was generated when the same text file was used to upload to the IPFS system to get the hash when it was run on the flask server. But the original hash was retrieved from the same file but whilst running the python script to generate IPFS hash independently. The observed difference in result may be a result in collision of modules or ipfsapi API issues. Either way IPFS are the way to go in the future.

Despite the known issues and compromises from using Blockchain technology for certification, the technology is still in its development. As more researches advance, the technology can be optimized and be more widespread than it already is. Until it tackles sensitive issues, it can be used to solve some general and domestic problems.

REFERENCES

1. Dawes, Sharon S. "Stewardship and usefulness: Policy principles for information-based transparency." Government Information Quarterly 27.4 (2010): 377-383
2. Christensen, Clayton M. (2003). The innovator's solution: creating and sustaining successful growth. Harvard Business Press. ISBN 978-1-57851-852-4.

3. Consensys (2015). uPort: The Wallet is the new browser. Available at: https://media.consensys.net/uport-the-wallet-is the-new-browser-b133a83fe73

4. Dawes, Sharon S. "Stewardship and usefulness: Policy principles for information-based transparency." Government Information Quarterly 27.4 (2010): 377-383.

5. Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., & Knight, E. (2015). Digital badges in education. Education and Information Technologies, 20(2), 403-410.

6. Hanson, R.T., Staples, M. (2017). Distributed Ledgers, Scenarios for the Australian economy over the coming decades. Canberra. Commonwealth Scientific and Industrial Research Organisation.

7. Jentzsch, C. (2016). Decentralised autonomous organisation to automate governance. Retrieved from https://download.slock.it/public/DAO/WhitePaper.pdf

8. MIT Media Lab (2016). What we learned from designing an academic certificates system on the Blockchain. Available at: https://medium.com/mit-media-lab/what-we-learnedfrom-designing-an-academic-certificates-system-on-the-Blockchain-34ba5874f196

9. Smolenski, N. (2016a). Academic Credentials in an era of digital decentralisation. Learning Machine Research.

10. Vigna, J. and Casey, M.J. (2016). The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order. Picador