International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

Digital Certification using Blockchain

Aditya Bhogate[1], Shashank Shetty[2], Prathamesh Vaste[3], Suvarna Aranjo[4]

[1,2,3]Student, Dept. of Information Technology , Xavier Institute of Engineering, Mumbai, Maharashtra, India
[4]Professor, Dept. of Information Technology, Xavier Institute of Engineering, Mumbai, Maharashtra, India

---

Abstract - *Fraudulent certificates are a major concern in the current educational and corporate territory. One can easily find several such online services simply via surfing the internet. Significantly, there are two things that are important with certificates. a) The authenticity of the document - Authenticity of the document ensures that the issued certificates are from the authorized institute. b) The trustworthiness of the document - Integrity of the archive guarantees that the given document isn't changed in any way. In the present method, genuineness is guaranteed after the engraved hologram of university certificates. It is expressed that duplication of the hologram is a troublesome errand to be conveyed by a typical printer. The whole concept of document authenticity is based on this assumption, but the real-life scenario is different. Eventually, recruiters are caught up in a web of fake certificates. Under this system of issuing digital certificates, the concerned university will have the authority to issue certificates for students and university graduates. The university will select the student database of records containing student information such as name, institution, degree, specialization, issue and discontinuation date along with the date of birth. For each student record, the application system will compute the hash of data and will create a new transaction using the authorized ethereum account to store it on the blockchain as an immutable record of student certificate.*

***Key Words*: ethereum, solidity, merkle Tree, cryptography, authenticity.**

1. INTRODUCTION

A blockchain is, inside the main of terms, a time-stamped arrangement of an immutable record of information that is overseen by the cluster of PCs not claimed by any single entity. Each of these blocks of data (i.e. block) is secured and sure to one another using cryptographic principles (i.e. chain). So, what's so special about it and why are we saying that it's industry-disrupting capabilities? The blockchain network has no central authority[1] — it is the very definition of a democratized system. Since it's a shared and immutable ledger, the knowledge in it's open for anyone and everybody to ascertain. Hence, anything that's built on the blockchain is by its very nature transparent and everybody involved is in charge of their actions. The blockchain may be a straightforward yet keen way of passing information from A to B during a fully automated and safe manner. One party through a transaction initiates the process by creating a block. This block is verified by thousands, perhaps many computers distributed around the net. The verified block is added to a sequence, which is stored across the internet, creating not just a singular record, but a singular record with a singular history. Falsifying one record would mean falsifying the entire chain in many instances. That is virtually impossible. Bitcoin uses this model for monetary transactions, but it is often deployed in many other ways. Now, this technology can be adopted and used to make certifications in colleges and universities for the following reason: Fake certificates is a major concern in the current world. Individuals can undoubtedly access fake certificates of major universities no problem at all. One will discover unlimited agencies offering fake certifications, credentials and that's only the tip of the iceberg. The people often take the assistance of those forged certificates for pursuing their education or for conducting their works. But the sad part is that they often get into wrong titles. The universities are facing this issue long ago with the inception of technology. Yet, no technical innovations made at that point to control or handle the fake documentation that was going on around. This is the rationale why our universities still uphold the normal practice of offering the earned credits or certificates in paper format. Even within the age of computers and internet technology, our universities stick to serving certificates within the paper model. Many universities consider this because of the best practice to validate and authenticate certificates.

2. PROPOSED SYSTEM

The proposed blockchain based certification system will help the university issue as well as store certificates securely on ethereum blockchain. These certificates can then be verified by the concerned personnel.

2.1 Issuing Certificate:

The university database containing the details of graduating students will be passed to blockchain application which will compute a secured 256-bit hash of each student information. A Merkle tree will be constructed by pairing these hashes and the Merkle root will be generated. The Merkle root will be deployed on the ethereum blockchain by issuing a new transaction through authorized ethereum account. This transaction will contain the Merkle root of all certificate hashes. A small amount of transaction fees will be deducted in the form of “ethereum gas”. The ethereum blockchain will retain an immutable record of the Merkle root and will distribute it to all the nodes in the ethereum network.

A JSON file will be generated that contains each student information and the SHA-256 hash will be computed off of this JSON file. This JSON file will be sent to each student and is used as a digital certificate to authenticate the student's degree/certificate.

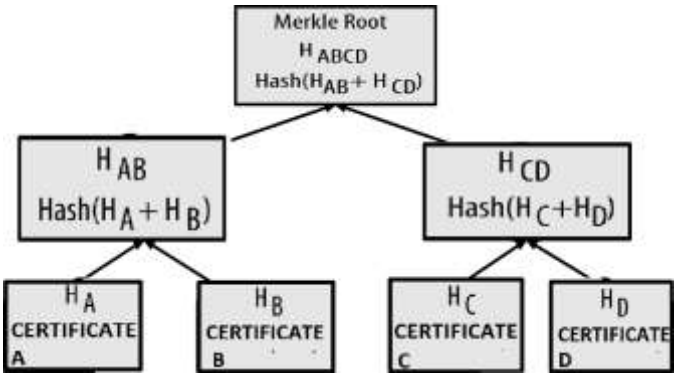

Fig 1: Merkle Tree of Certificates

Fig 2: Generated Merkle Root

2.2 Verifying the Certificate:

The students and concerned people will be provided with a portal to verify the JSON certificates given to them. Each JSON certificate will contain the Merkle root that it belongs to and the Merkle proof to verify the same. The verification is a two-step process i.e. at the client and on ethereum blockchain. When any student enters his or her JSON certificate into the portal the hash of the metadata of student information will be completed which can then be used to verify the certificate by reconstructing the Merkle root using the respective Merkle proofs. After verifying the Merkle root at the client end a function call will be made to the smart contract which will return a flag indicating the authenticity of the certificate.

Fig 3: Digital Certificate as JSON File

2.3 Revoking Certificate:

If the university decides to revoke a certificate the university will have to issue a new transaction containing that certificate and the hash of the certificate will be stored in the list of revoked certificates on the ethereum blockchain. Whenever a student gets on the portal and enters his or her certificate, before verifying the authenticity of the certificate. Another function call will be made to check the revocation status of that certificate. In case the revocation status is true the certificate will be considered as invalid or if the status is false then a normal verification process will be followed.

3. CONCLUSION

The project outline aims at the betterment of the existing system of issuing educational certificates by colleges in India. We have recognized the flaws and the long-prevailing issue of fake certificates. We aim at changing the current situation with the help of blockchain technology. The paperback certificates will be transformed into digital certificates, which even if forged cannot be issued without the issuer being from the issuing institute itself. The verification of these certificates is also easier as the verifier only has to check whether the certificate exists in the blockchain or not. Which is comparatively easier than the conventional method of verification. Carrying certificates around is no longer a job to be remembered as it is on the network and always online. This also reduces wear and tear of the certificates.

REFERENCES

[1] Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System, 2008

[2] Vitalik Buterin "Ethereum White Paper"

[3] Alyssa Hertig "How Do Ethereum Smart Contracts Work? ", 2017.

[4] Arvind Shukla, "Watch out for fake degrees", 2016.