Certificate Bank

Group Name : Arcadia Bay

Members:

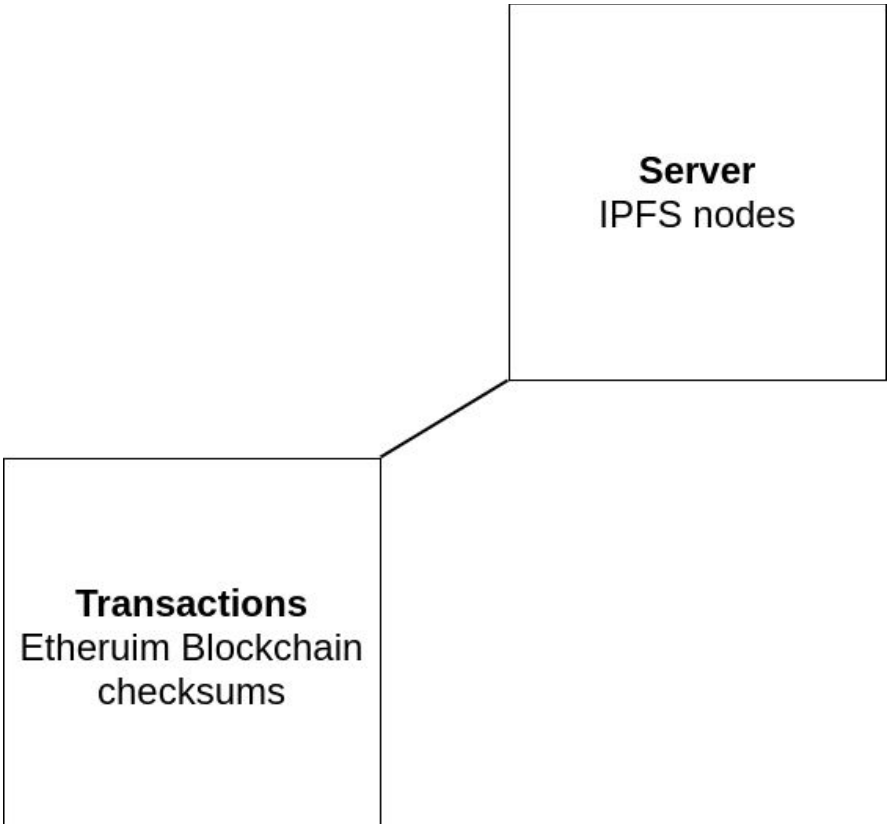
Ritwik Saha (ritwik.saha)
Hrishikesh Sagar (hasagar97)
Hrushikesh Sarode (hrishi32)

Problem

In today's scenario, there is no means to verify whether a degree, achievement or any type of accomplishment mentioned by any person in his resume or LinkedIn. Also documents storage and retrieval services like DigiLocker are not used widely and being centralized, they have a single point of failure. A massive hack or DDOS attack can bring the service to its needs. Also, services like DigiLocker are valid in specific portions of the world, like India and lack international recognition and acceptance. Additionally, only centrally approved institutions have rights to issue their documents on such services. If we can come up with a foolproof, widely recognized, always up, highly scalable, cheap service to hold educational and other certificates, in a way such that any potential employer can verify the potential employee's certificate's originality, it will be a huge feat. We are aiming to use Decentralized Storage and immutable information storage systems like blockchains.

Working

We have Two ways which when combined make a foolproof system that saves and protects a certification while also guaranteeing it's originality.



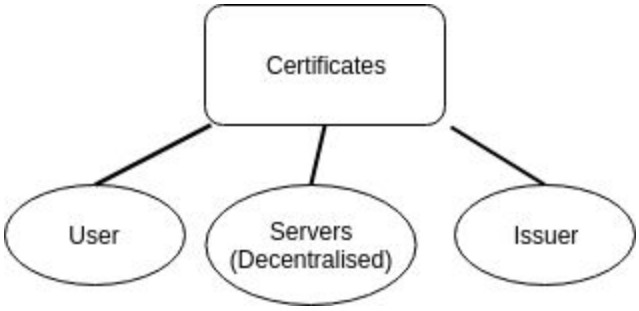
1. **Ethereum chain**: The issuer will have its own ethereum address and so will the candidate of certificate. Each Certificate when checksummed using any algorithm like MD5 or SHA2 produces a unique number which can't be generated from any other certificate. We store this checksum on ethereum blockchain. All transaction and data on blockchain can be retrieved easily and the checksum can be used to establish the originality of the certificate. The source of the certificate can be easily checked as a database will be maintained linking issuers to their corresponding ethereum address. Transactions being on ethereum give us power to store data till eternity.
2. **Data Storage and Servers**: The Data stored and Servers will be decentralised using IPFS technology which enables us to work on different servers set all over the world. The IPFS nodes will be set up by various contributors which will mainly be organisations like Stanford, Google, Amazon as they are major issuers of certifications.

Data Storage of Certificates:

The certificates will be stored on 3 major places

1. Our IPFS servers
2. User
3. Issuer

Also we will have backups that will ensure safe storage of data.



In Case of Data loss

Assuming that all of of servers fail and we also lose backups(Probability of which is negligible) an user and an issuer will have their copies which when checksummed by our algorithm will generate the unique checksum that is saved on the blockchain. Thus genuinity is established.

Why No forgery is possible?

As the certificates given by the issuer will directly enter into Blockchain Ledgers with checksums, any changes made to the certificate will result in a different checksum value and the forgery will be detected. Also, each issuer will have a unique ethereum address registered and certificates originating from other addresses can be dropped from consideration.

Integrity of Issuers

There will also be a ranking systems for issuers so that fake organizations do not pop up start issuing certificates with no practical value. For example organizations like Stanford etc. will have high ratings while local institutes may not have that much importance.

What a user can control?

The user can provide links to transaction IDs, these IDs will have checksums as additional data which can be used to look up certificates on our website. A checksum will display the authentic certificate if and only if the Viewer has view permission from the owner. Also the user can control who sees his certificates.