the roles in degree certification system

The degree certification system mainly consist of 4 roles, there are User, Authority, Verifier and IPFS.

User: the role that own the information of the degree certification

Authority: the role that protect the information privacy, ensure the truth of the information.

Verifier: the role that will verify the authenticity and existence of the degree certification.

IPFS: the role that store the degree certification information

process:

First step: the store step

the user need to register into the system, and tell the system of a true identity of users' individual information, then match against the authority's information. So, the User register with a groundtruth information into an Ethereum system. Then the system construct a smart contract, and the user can manage the data access with the smart contract.

in detail

1. the user will store the degree certification into a personal repository in IPFS, even more, it can be encrypted for security. The IPFS will give the user a hash ID, and the user will user it to retrieval the degree certification in IPFS.

2. the authority combine the user's information and the hash ID, then hash it using hash algorithms(SHA256), and stored into the Ethereum's blockchain. The authority also sign the hash value using its own private key, and public the public key. The public key will be recorded in PKI infrastructure, making it verifiable and traceable.

3. the system will create a smart contract. The contract's owner is the authority, and initially create the user account for authority and the user. Both authority and the user have their own account in smart contract. The smart contract give the user ability to control the data access(Such as give the verifier accessment to the data). The authority can also disable the smart contract in some case.

Second step: the control step

the user will use the smart contract to access control management. When the user access the smart contract, the system will verify the user account address. After enter the smart contract, the user can add some user accounts(Such as the verifier's account) who can read the data. The user can also specify the how long a user can access the data or how many times can a user access the data.

Third step: the verify step

1. the user will provide the degree certification and the IPFS hash ID, the verifier will use this ID to access the IPFS to verify these two degree certification is the same.

2. the authority will also need to verify the owner of the degree certification is the right person. So the verifier will access the user information through smart contract(because in second step, the user give the verifier to access the data). The verifier will combine the user information and the IPFS hash value into a new hash value using the same public key of authority. Then the verifier will verify that if the hash value occurred in the blockchain. If the hash value exist in the blockchain, it prove that the owner of the degree certification is the user indeed.