Certist is composed of a 3 components.

1. Backend API

The backend API is mainly used to retrieve and write data on the Ethereum block chain.

2. Frontend

The frontendhandlesinteractionswiththebackendandtheuserinteractionswiththeCertistapp.

3. Smart Contract

Our Ethereum Smart contract is the mechanism that is used to store and verify diplomas and certifications on the block chain.

The users cryptographic keys are generated when the app is launched for the first time, then encrypted and safely stored in the device for later use. The key generation seed is then displayed so users can create a safe backup in case of a loss of keys or devices.

The issuers can issue diplomas by creating an Ethereum transaction and writing the necessary data in the transactions o the data is stored in the contract. Some smart contract functions can only be called by specific keys, this is designed so that only verified issuers are able to issue new diplomas or certificates.

The documents are uploaded to a decentralized storage platform (IPFS), the IPFS hash is then written to the contract.

'''

addresspublicowner;

functionowned() {

owner = msg.sender;

}

modifieronlyOwner {

if (msg.sender != owner) throw;

\_;

}

'''

Verifications can be done through the QR code or permalink provided by the Certist app for every diploma or certificate the user has. The verifiers can see the relevant information that confirms the issued diploma or certificate is genuine and authentic. Diplomas and certifications are retrieved by calling the smart contract upon request.