Certify.

Creating Decentralised Certificates

01

Harsh Prakash
Jayesh Bhole

Introduction

02

WHAT ARE CERTIFICATES?

- Proof of Authenticity
- Proof of Truth/Fact
- Proof of Skill
- Proof of Identity

Introduction

02

ISSUES WITH CENTRALISED CERTIFICATES??

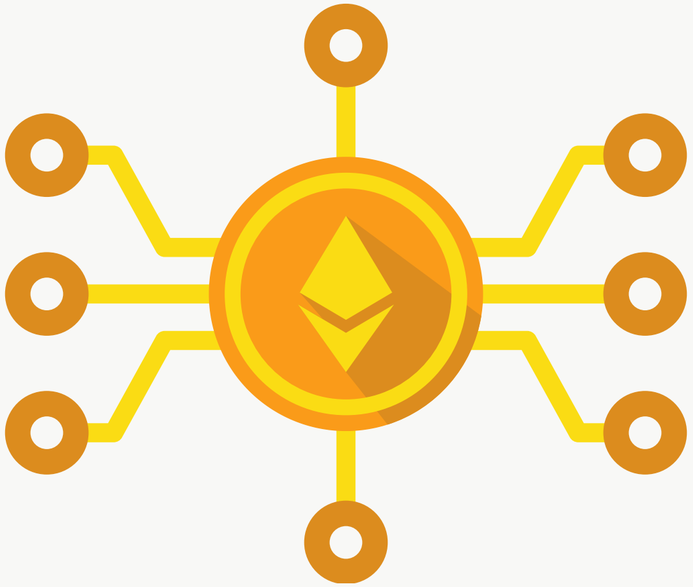
- Forgery
- Corruption
- Privacy
- Trust

Introduction

02

PROS OF DECENTRALISED CERTIFICATES

- Immutable
- Secure
- Privacy
- Trust-less
- Open Source



03

Solution

DAPP

A Decentralised Application

CUSTOM FORMATS

Customisable fields

ENCRYPTION

Protecting Privacy

TRUST-LESS

No Central Authorities or regulatory bodies

SCALABLE

Handle increasing traffic over time

OWNERSHIP

Partial ownership to the issuing authority

Literature Survey Summary

Design Requirements

MIT MEDIA LAB	Offers control to students	Authorisation	Ownership	Privacy
BLOCKCERTS	Based on Open Platform	No Authorisation	No Ownership	No Privacy
SMARTCERT	Solves Fake Certificate Issue	Authorisation	Shared Ownership	No Privacy

Proposed Work

04

WEB 3.0 APP

To provides interface for the smart contract.

SMART CONTRACT

Solidity smart contracts to store hash maps and write data to the blockchain

IPFS STORAGE DESIGNS

Optimised storage designs to satisfy all the storage needs

Proposed Work

04

WEB 3.0 APP

To provides interface for the smart contract.

Interact with smart contract

Connect to Celo wallets - MetaMask / WalletConnect

Encrypt data

Create transactions

Fetch data, Decrypt and Display

Proposed Work

04

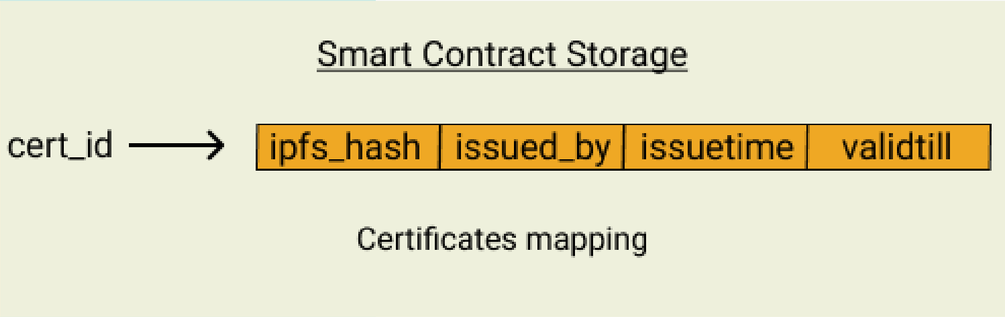
SMART CONTRACT

Solidity smart contracts to store hash maps and write data to the blockchain

Interact with the blockchain

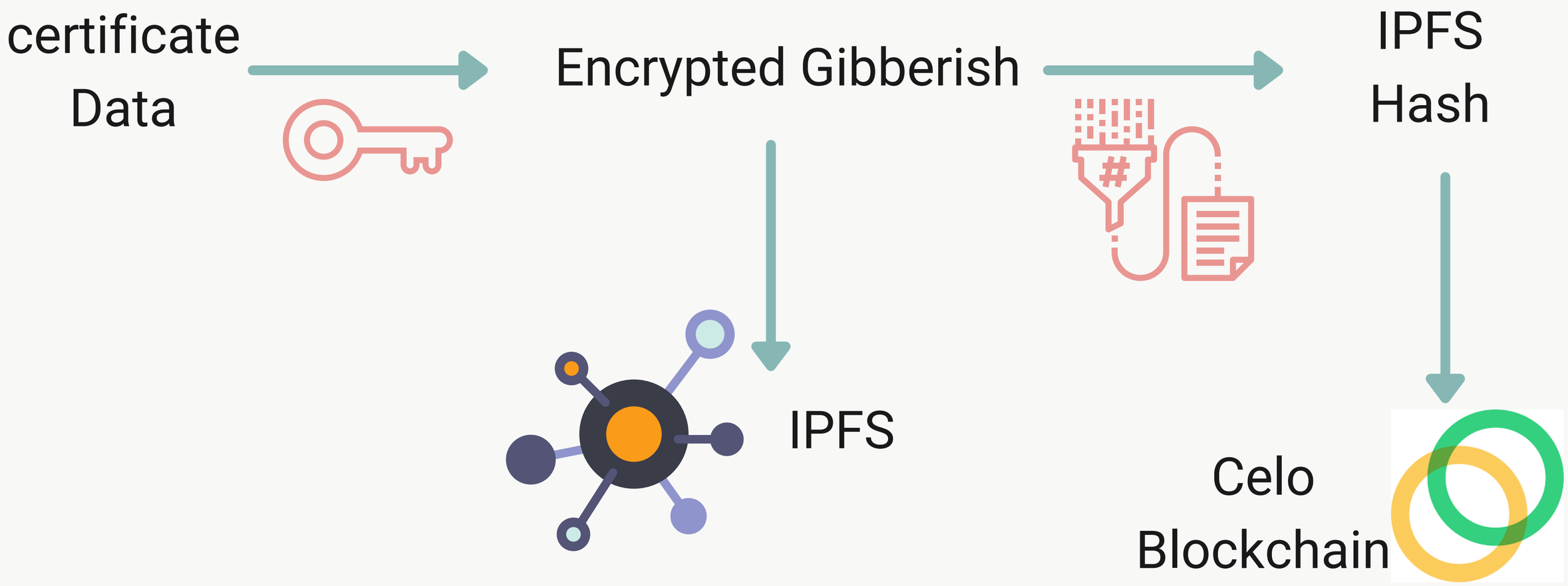
Store IPFS hashes in a map

Serve data when requested

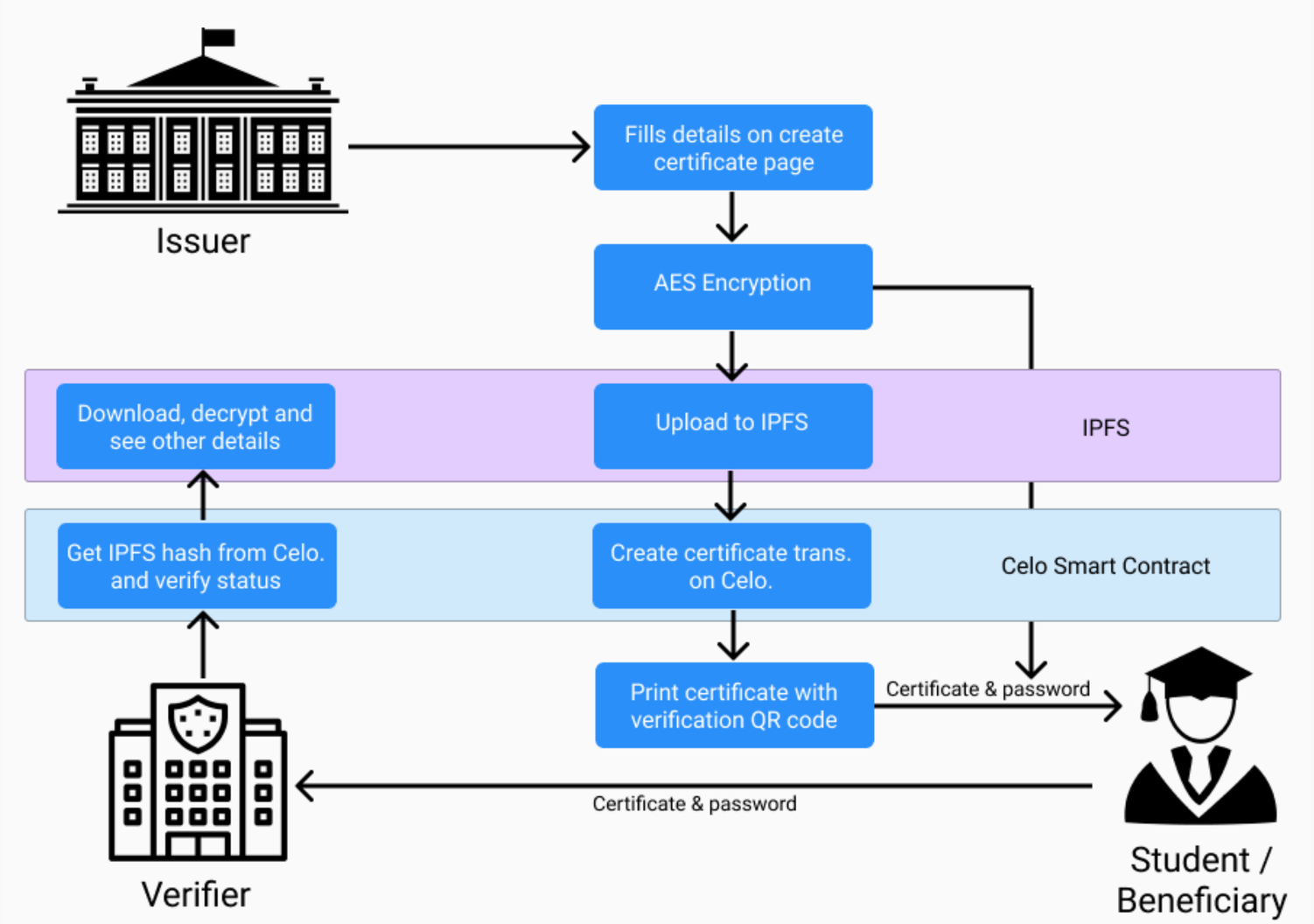


Proposed Work

04

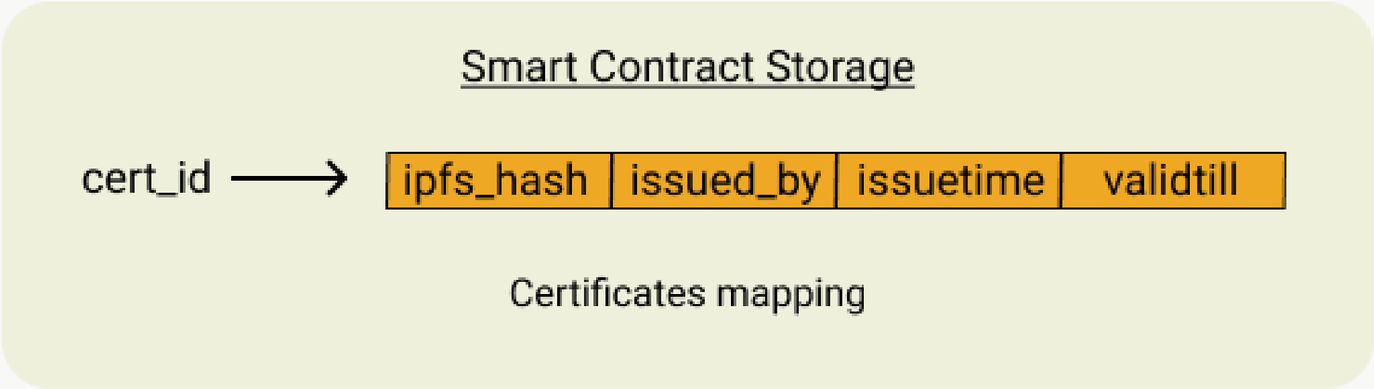


Designs


Issuer
Fills details on create certificate page
AES Encryption
Download, decrypt and see other details
Upload to IPFS
IPFS
Get IPFS hash from Celo. and verify status
Create certificate trans. on Celo.
Celo Smart Contract
Print certificate with verification QR code
Certificate & password
Certificate & password
Verifier
Student / Beneficiary

Designs

05


Smart Contract Storage
cert_id
ipfs_hash
issued_by
issuetime
validtill
Certificates mapping

Progress

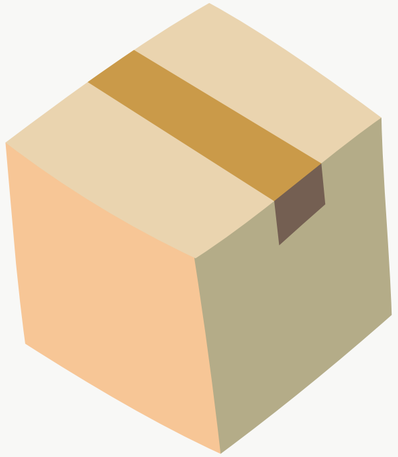
06

STEP 1

Research. Design. Ideating and Optimising.

STEP 2

Prototyping an easier concept.

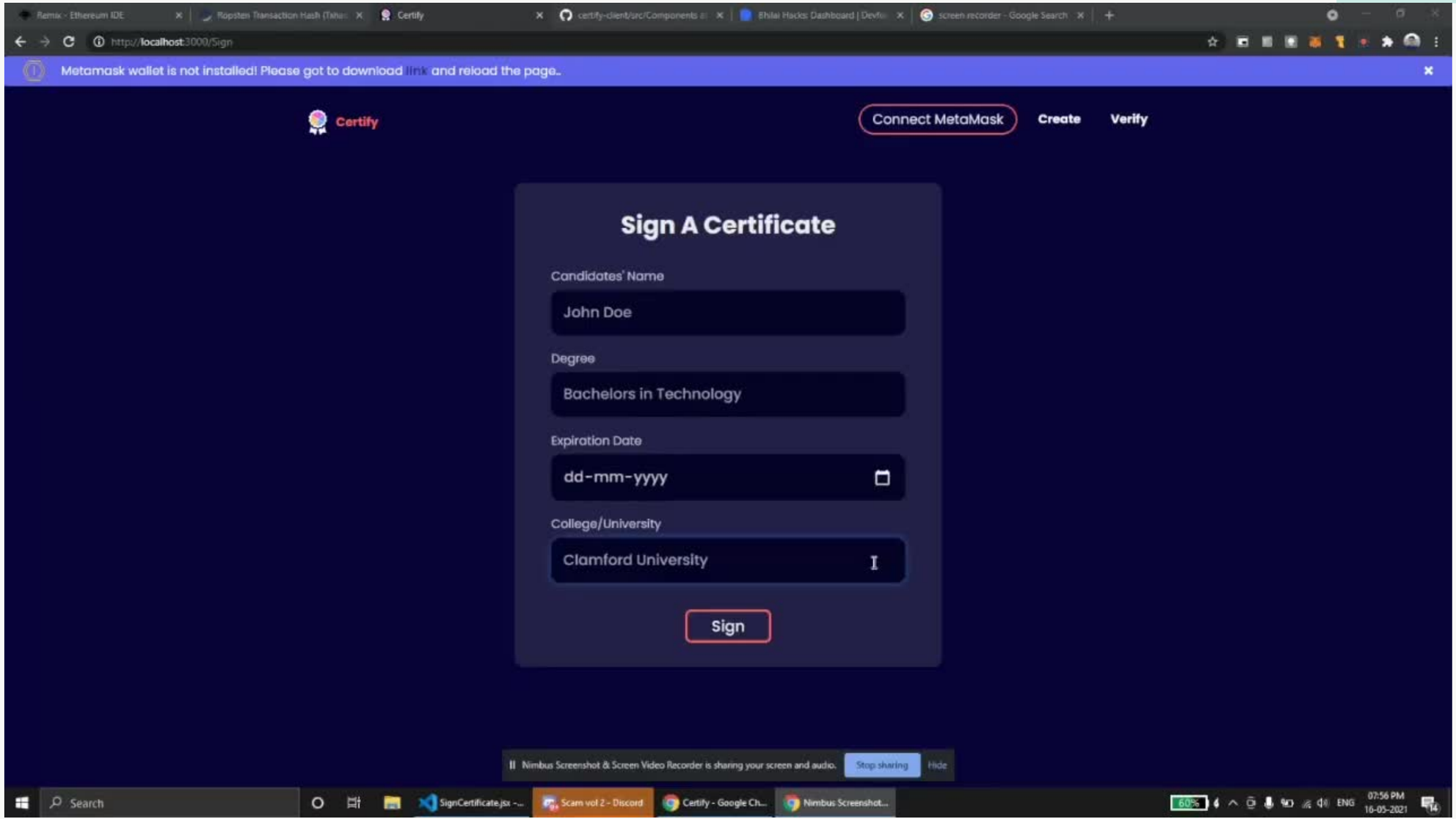


STEP 3

Creating the final product.

Prototype

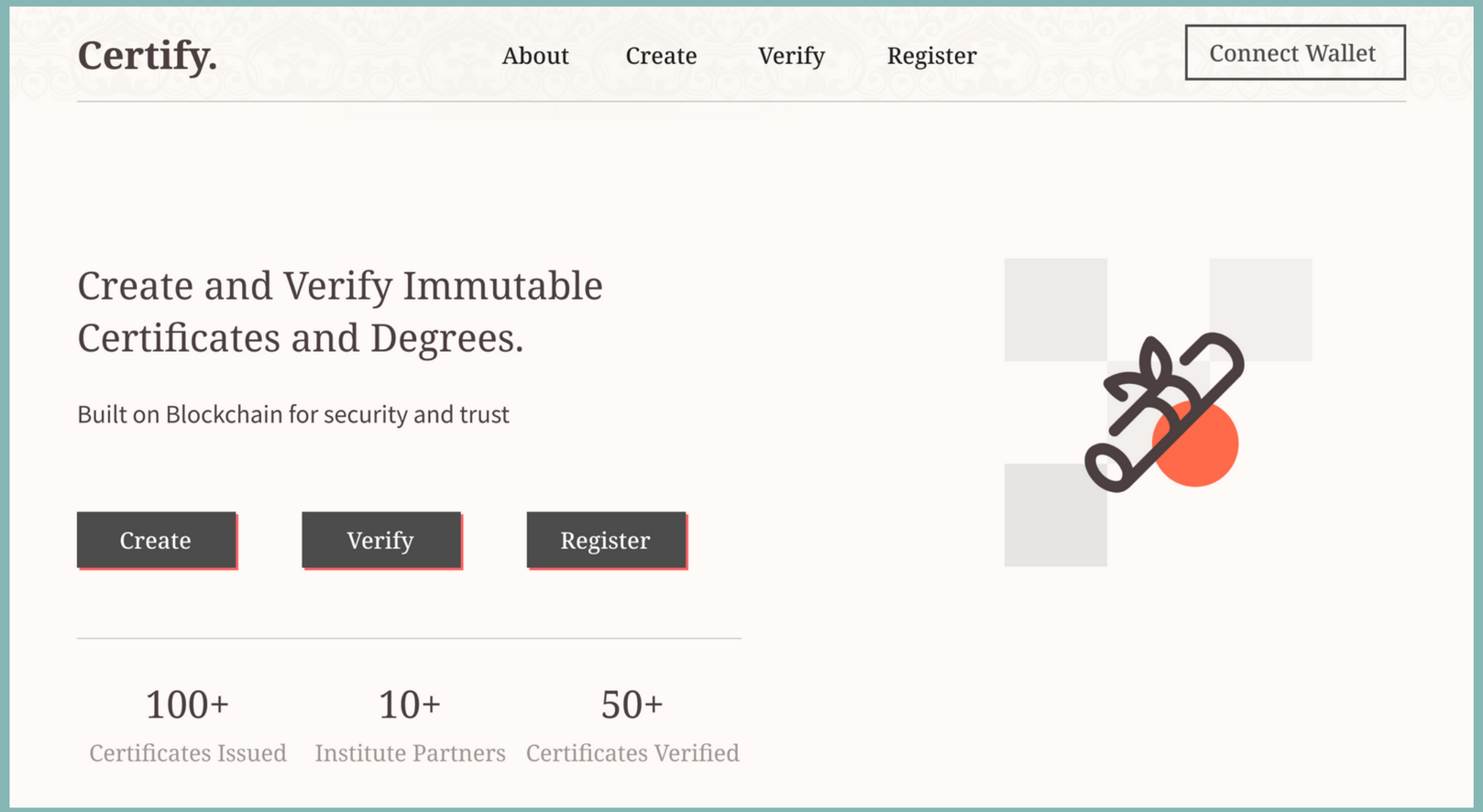
07



Product - Certify

08

Create and Verify Certificates on the Celo blockchain



Product

08

Single Page Application

Robust UI

Create and Verify Certificates

Completely Decentralised

Private & Secure

Certificate

This certificate is presented to **John Doe**

For

Changing Certificate Status

By

Certify Platform

Additional Information

Expires on : 19/11/2021

Note :
This certificate is generated to test the status and actions.

Issuers Address :
0x0b90994F83D2Fde68f83C418141B42550dE2Cb4c

Created On : 11/11/2021

IPFS Hash :
bafkreiczmoae4uqremowwqgbweb57idjttcefh7hmnz26ha7tbozobjox4

Certificate Status

Verified

Scan to share

https://certify-v2.netlify.app/verify/?ipfsHash=bafkreiczmoae4uqremowwqgbweb57idjttcefh7hmnz26ha7tbozobjox4&certkey=BD2GD7849

08

Issue Certificates

Issue certificates with the form manually or import CSV files. Fill out the adjacent form and create a new certificate.

Pay minimal transaction fee and get a copy of the certificate Hash.

Refer to the CSV file format below before importing data.

Beneficiary Name

Certificate Description

Expiritation Date

Institute/Authority Name

Additional Notes

Issue Certificate

Import CSV

Import a CSV file with the format as shown in the adjoining figure. The web app will generate a batch of transactions for the certificates.

A batch of only 100 certificates can be imported.

Download the certificate hash CSV file for future references.

Beneficiary Name	Description	Expiration Date	Institute Name	Additional Notes

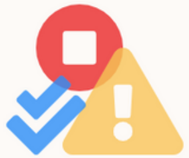
Import CSV

Actions

Actions allow users to mutate the certificate status. They can either be **Revoked** or **Reinstated**

Only certificates belonging to the users address will be revoked/ reinstated.

Encryption key is needed to perform any action.



Revoke Certificate

Revoke existing certificates by filling out the adjacent form.

This action is reversible.

Reinstate/ extend the validity of a certificate using the form below.

Transaction gas charges are applied.

IPFS Hash (Address)

Certificate Key

Revoke Certificate

Reinstate Certificate

Certificates can be reinstated using the adjacent form.

Reinstating certificates only extends the expiration date and nothing more.

Transaction gas charges are applied.

IPFS Hash (Address)

New Expiry Date

dd/mm/yyyy

Certificate Key

Revoke Certificate

Future Scopes

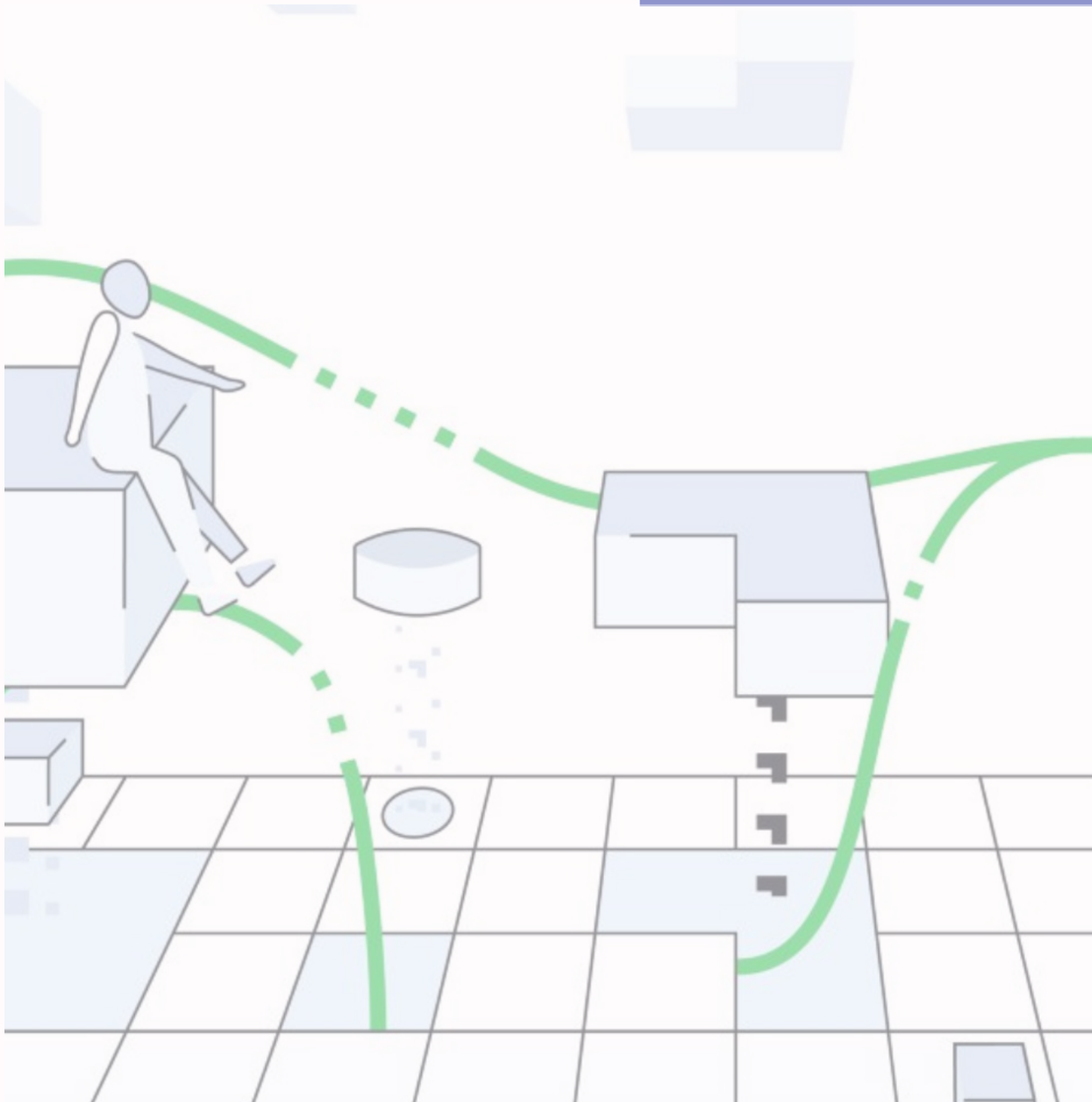
09

Issue Identity Certificates like driving license, Passport, etc.

Decentralised API - The Graph protocol

Zero Knowledge Protocols for Identity based Applications

Batch Transactions And Mass Actions



10 References

- Gilles Grolleau, Tarik Lakhal, and Naoufel Mzoughi. “An Introduction to the Eco-nomics of Fake Degrees”.
- Omar S. Saleh, Osman Ghazali, and Norbik Bashah Idris. “A New DecentralizedCertification Verification Privacy Control Protocol”.
- Juan Benet. “IPFS - Content Addressed, Versioned, P2P File System”.
- Vitalik Buterin et al. “A next-generation smart contract and decentralized application platform”.

Thank you!