BLOCKCHAIN BASED E-CERTIFICATION

B.S. (SE) Final year project proposal

Muhammad Rafay	17B-008-SE
Muhammad Aamir	17B-034-SE
Hassan Ahmed Siddiqui	17B-049-SE
Muhammad Sabih	17B-058-SE
Muhammad Ismail	17B-062-SE

Batch: 2017-2021

Date: 13-11-2020

DEPARTMENT OF COMPUTER SCIENCE

USMAN INSTITUTE OF TECHNOLOGY

Usman Institute of Technology
Department of Computer Science

FINAL PROJECT APPROVAL FORM

The Head of Department,
Computer Science Department,
Usman Institute of Technology,
Karachi.

Date: 13-11-2020
Batch: 2017-2021

Subject: **Bachelor of Science in Computer Science/Software Engineering Final Year Project**

Respect Sir,

We, the below listed students of final Year BS SE-A class, desire to undertake work on the following project.

Blockchain Based E-Certification

We request you to kindly grant approval for undertaking the work on the above-cited project. I abide by all terms and conditions mentioned below.

1. I have selected this project on my own.
2. I have no objection working under the supervision of male/female supervisor, or if my project work is evaluated by male/female externals.
3. I am sure I can complete this project till June 2021.
4. I am eager to work under the supervision of advisor assigned to this project.
5. I understand that FYP committee can modify the scope of the project as and when required.
6. I know that if do not appear in regular project progress presentations/milestones my project will be disqualified.
7. I know that if I do not appear in mid project presentation, whenever it is scheduled, I will not be eligible for final project viva.
8. I fully understand that "***cheating***"* may lead to cancelation of my project.
9. I understand that the decision of the FYP evaluation committee, for all issues, would be final, and no objections will be accepted.
10. I have no objection presenting my project to external or internal examiner assigned by the Head of the Department.
11. Project and Product deliverables at the time of submission of final year project every group is responsible to submit complete running system along with printed reports, source code, hardware (if any) etc to the project coordinator.
12. It would be the responsibility of Project coordinator to keep record of all projects in a system (in running form) as it would help to continue next project in continuation, depends upon the scope and application of project.
13. Proper dressing and way of presentation should be in English during proposal defend session, milestones and final presentations.
14. Marking of milestones and final presentation should be based on individual evaluation of each faculty members and marks would be granted during session.
15. When we go for proposal defends session a list of all previous projects with their brief introduction must be available during session for our reference. (Introduction, Scope of project, tools and technology and batch must be available).

16. I understand that it is my responsibility to update my advisor and FYP committee members with the status of my project and submit reports on time.
    - Copying code from any resources
    - Using off the shelf components without prior permission
    - Outsourcing your project
    - Hire a resource for the completing the FYP code or any part of the project.

Yours sincerely,

S.No	Roll No.	Name	Email	Signature
1.	17B-008-SE	Muhammad Rafay	17B-008-SE@students.uit.edu	
2.	17B-034-SE	Muhammad Aamir	17B-034-SE@students.uit.edu	
3.	17B-049-SE	Hassan Ahmed Siddiqui	17B-049-SE@students.uit.edu	
4.	17B-058-SE	Muhammad Sabih	17B-058-SE@students.uit.edu	
5.	17B-062-SE	Muhammad Ismail	17B-062-SE@students.uit.edu	

TABLE OF CONTENTS

Project overview

The problem is that different certificates like events, courses, health, etc. are issued to the people from different organizations. But in case of any mishaps (natural disaster, snatching, etc.) person might lose his/her certificate, Sometime the organization shift the platform so it is very difficult process to get that certificate again due to lots of hurdles, verifying those certificates is really big issue, some time it is not possible due to lack of backup and sometime if it is possible so it is very time consuming and costly process also preparing and distributing those certificates manually is so much time consuming. There is an international company named as accredible that has developed the same idea but for the verifiability & security purposes they are using bitcoin blockchain technology. while in our solution we are using hyper ledger fabric, which is a consortium block chain, so no unauthorized entity can read or write the data. We are providing a platform to issue e-certificates with some customization like adding logos, fields, etc. and also providing a way to verify the issued certificates to make the transparency of data & make the data available to other users for verification purposes we are using block-chain and if there is any data loss by some of the entity than other entities part of the network can still able to verify the certificates generated by that entity. Only authorized organizations can participate in hosting this network of blockchain & allowed to make transactions.

Project objectives

We are providing a platform of blockchain based e-certification which provides a way to verify the certificates not only by the certificate generating entity also by other users (either the part of any entity in the network or not) and in case any entity loss their data or change their platform then the certificates issued by them will be still verifiable.

The Blockchain based e-certification project will meet the following objectives:

- Provide platform for verifiability of certificate.
- No certificate loss or any data loss due to any mishap.
- Temper free securable environment.

Project scope

- Creation of temper free & verifiable certificates using blockchain technology.
- Any organization can join a blockchain network by deploying nodes.
- Organizations hosting the blockchain network can provide services to others.

In scope:

- Provide a platform for the organization to host the network.
- A platform for providing services (Client-Organizations).
- Organizations that deploy blockchain nodes will have a separate server, handling its web applications and have a super admin account.
- Client-organization has a simple admin account to manage their users.
- Allowing to create batches and add certificates in it.
- Updates to certificate data are only allowed before committing to the blockchain.
- Allowing to publish certificates to the blockchain network.
- Certificates will be verifiable from any of the organization's websites after publishing to the blockchain.
- Only super admin and admin are allowed to reset the password.
- Super admin can enable/disable client-organizations, its users & the users of his own organization.
- Enable users to recover certificates via email.
- In case of attack they can re-sync their nodes again with the blockchain network but local database data is only recovered through backups or if there are any replicas deployed.

Out of scope:

- Issuing illegal certificates.
- Uploading of invalid logos & signatures.
- Any kind of data loss on the local database in case of any attack on its site.

- In case of any conflicts with client organizations.

Deliverables produced

Following are the deliverables of our project:

According to Milestone

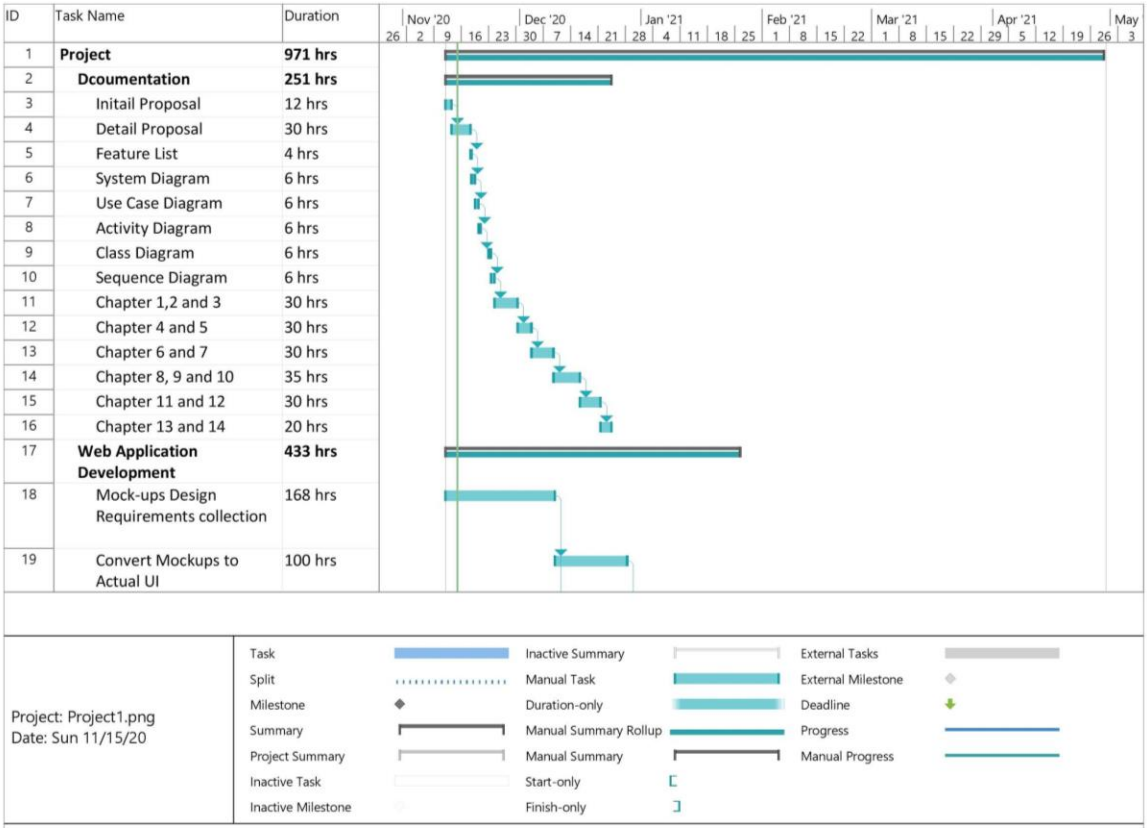
- **Project Deliverable 1:**
  - Project Proposal.
  - Gantt Chart.
  - Brief analysis of FYP outcomes.
  - Software / Hardware Requirements.
  - Mockups (Screenshots).
  - System Diagram.
  - Feature List.
  - Chapter 1, 2, 3 and 4.
- **Project Deliverable 2:**
  - Class Diagrams.
  - Complete Front End Application.
  - Sequence Diagram.
  - Chapter 5 and 6.
- **Product Deliverable 1:**
  - Component Diagram.
  - Deployment Diagram.
  - Unit Testing.
  - Integration Testing.
  - Load Testing.
  - Deployment Architecture and Strategy.
  - Complete Project in true running condition as stated in project scope document, with test results, setup and project deployment kit (in DVD).
  - Chapter 7, 8, and 9 submission and presentation to be submitted on the 4th week of 8th semester.
  - Chapter 10, 11, 12, 13, and 14 to be submitted on the 12th week of 8th semester.

Project estimated effort/cost/duration

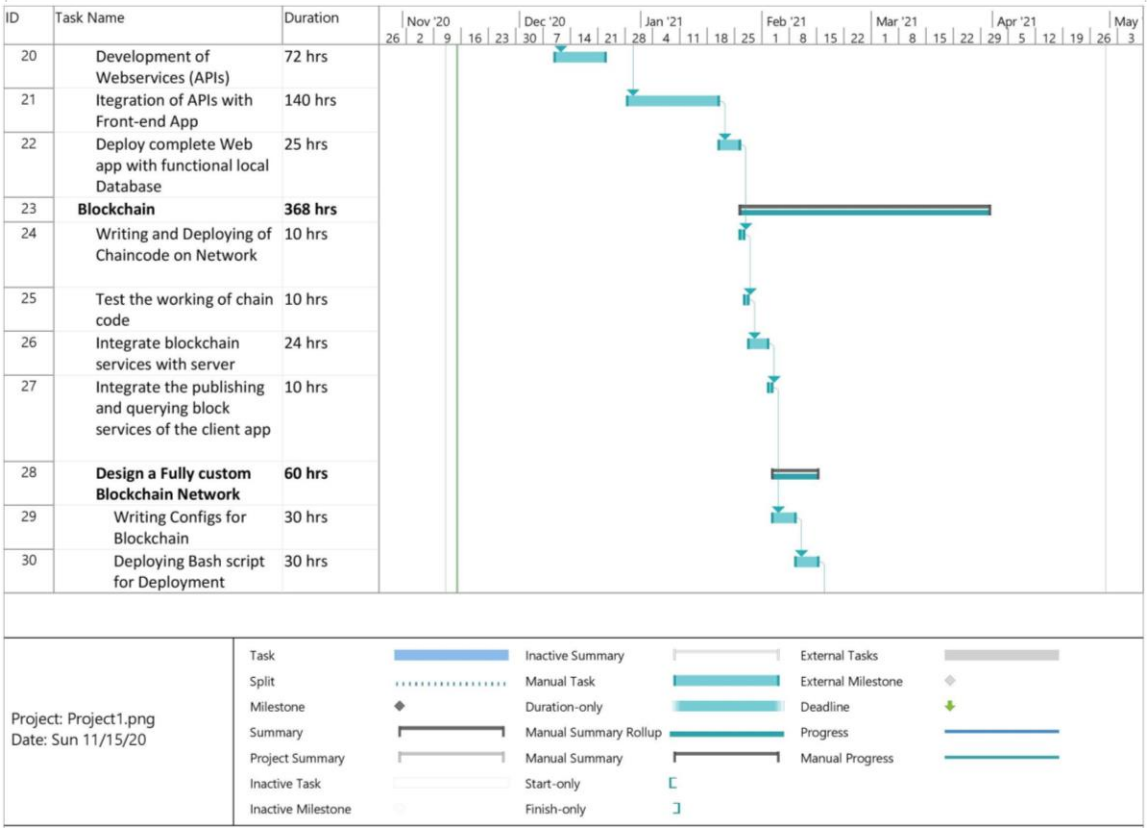
- **Documentation:**
  - Initial Proposal (12 hrs).
  - Detail Proposal (30 hrs).
  - Feature List (4 hrs).
  - System Diagram (6 hrs).
  - Use Case Diagram (6 hrs).
  - Activity Diagram (6 hrs).
  - Class Diagram (6 hrs).
  - Sequence Diagram (6 hrs).
  - Chapter 1,2 and 3 (30 hrs).
  - Chapter 4 and 5 (30 hrs).
  - Chapter 6 and 7 (30 hrs).
  - Chapter 8, 9 and 10 (35 hrs).
  - Chapter 11 and 12 (30 hrs).
  - Chapter 13 and 14 (20 hrs).
- **Web Application Development:**
  - Mock-ups design for requirement collection (168 hrs).
  - Convert mockups to the actual UI (100 hrs).
  - In Parallel with UI development, development of web services (APIs) (72 hrs).
  - Integration of APIs with the front-end app (140 hrs)
  - Deploy the complete web app with a local database fully functional (25 hrs).

- **Blockchain:**
    - Writing and deploying chaincode on sample network (10 hrs).
    - Test the working of chain code (10 hrs).
    - Integrate the blockchain services with the server (24 hrs).
    - Integrate the publishing and querying block services with the client app (10 hrs).
    - Design a fully custom block chain network.
        - Writing configs for blockchain (30 hrs).
        - Developing bash scripts for deployments (30 hrs).
    - Install the previously developed chaincode with that network (20 hrs).
    - Deploy the blockchain on a multi host environment (100 hrs).
    - Require changes in scripts on multi host environments to development of scripts (24 hrs).
    - Test the complete multi host network with the system (10 hrs).
    - Write scripts to add new peers in current organizations (30 hrs).
    - Write scripts to setup and add new organization to the current channel (70 hrs).
- **Testing:**
    - UI Testing (20 hrs).
    - Black Box Testing (30 hrs).
    - White Box Testing (30 hrs).
    - Load Testing (30 hrs).
    - Unit Testing (30 hrs).
    - Integration Testing (30 hrs).

GANTT Chart:

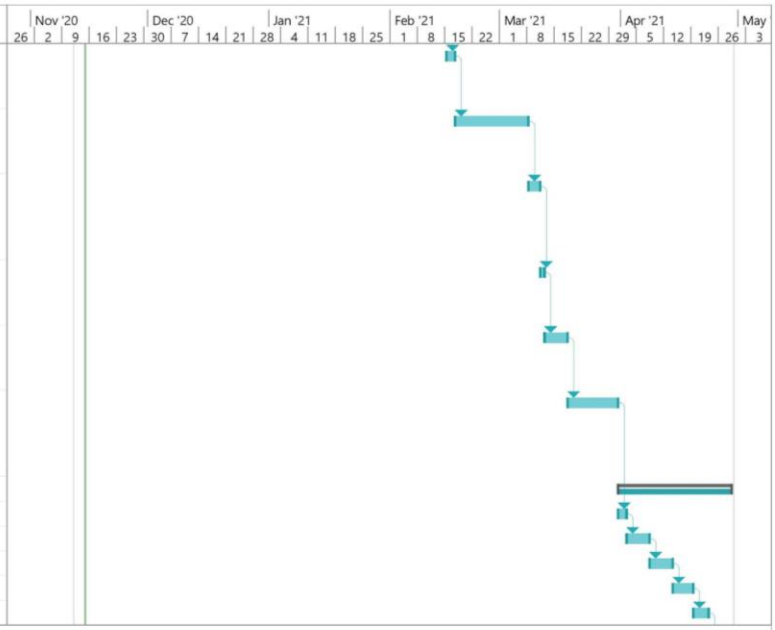


ID	Task Name	Duration
1	**Project**	**971 hrs**
2	**Dcoumentation**	**251 hrs**
3	Initail Proposal	12 hrs
4	Detail Proposal	30 hrs
5	Feature List	4 hrs
6	System Diagram	6 hrs
7	Use Case Diagram	6 hrs
8	Activity Diagram	6 hrs
9	Class Diagram	6 hrs
10	Sequence Diagram	6 hrs
11	Chapter 1,2 and 3	30 hrs
12	Chapter 4 and 5	30 hrs
13	Chapter 6 and 7	30 hrs
14	Chapter 8, 9 and 10	35 hrs
15	Chapter 11 and 12	30 hrs
16	Chapter 13 and 14	20 hrs
17	**Web Application Development**	**433 hrs**
18	Mock-ups Design Requirements collection	168 hrs
19	Convert Mockups to Actual UI	100 hrs



ID	Task Name	Duration
20	Development of Webservices (APIs)	72 hrs
21	Itegration of APIs with Front-end App	140 hrs
22	Deploy complete Web app with functional local Database	25 hrs
23	**Blockchain**	**368 hrs**
24	Writing and Deploying of Chaincode on Network	10 hrs
25	Test the working of chain code	10 hrs
26	Integrate blockchain services with server	24 hrs
27	Integrate the publishing and querying block services of the client app	10 hrs
28	**Design a Fully custom Blockchain Network**	**60 hrs**
29	Writing Configs for Blockchain	30 hrs
30	Deploying Bash script for Deployment	30 hrs

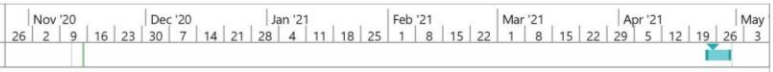
ID	Task Name	Duration
31	Install the previsouly Developed Chaincode with Network	20 hrs
32	Deploy Blockchain on multi Host Environmment	100 hrs
33	Require Changes in script on Multi Host Environmet so development os scripts	24 hrs
34	Test the multi Host Network with the System	10 hrs
35	Write scrpits to Add new peers in current Organizations	30 hrs
36	Write new scripts to setup and add new organization to the current channel	70 hrs
37	**Testing**	**170 hrs**
38	UI Testing	20 hrs
39	Black Box Testing	30 hrs
40	White Box Testing	30 hrs
41	Load Testing	30 hrs
42	Integration Testing	30 hrs



Project: Project1.png
Date: Sun 11/15/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

ID	Task Name	Duration
43	Unit Testing	30 hrs



Project: Project1.png
Date: Sun 11/15/20

Task
Split
Milestone
Summary
Project Summary
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
External Tasks
External Milestone
Deadline
Progress
Manual Progress

Estimated effort hours:
The estimated project effort hours are 971 main hours.

Estimated duration:

Milestone	Date completed	Deliverable(s) completed
Project planning		
Milestone 1	12/18/2020	• 50% running Project • Front end Mock-ups
Milestone 2	01/22/2021	• 100% running Project
Milestone 3	03/19/2021	• All Chapters • UML Diagrams • Testing
Milestone 4	05/14/2021	• All Testing Report • Deployment kit in DVD
Project conclusion	05/24/2021	• Poster Session

Project assumptions

- Organization should monitor its users' activity.
- Organizations should have secure IT infrastructure like firewalls, unused ports blocking etc.
- Organizations should provide the services only to the trusted & recognized clients.
- Organizations should have skilled operations teams to update their client and backend servers from our repos.
- Organizations should approve valid requests for different proposals for channels, chain code, adding peers etc.

Project risks

Risk Area	Level (H/M/L)	Risk Plan
1. Deployment of production ready blockchain network	H	Deployments of multiple test networks on single & multi host environments & testing its reliability & security, extensive training of team for deployments.
2. Availability of hardware	H	We can handle this by deploying nodes on virtual machines and containers.

Project approach

We are using a waterfall model. Each phase must be finished before the next phase can begin and there are no unclear conditions in our project. At the conclusion of each phase, a review takes place to decide if the project is on the right direction or not. Every week we schedule 2 meetings with our supervisor for discussing problems whether they are technological or non-technological and also discuss our future plans for clearing any types of misunderstanding and problems. Below is the list of tasks that we are going to perform in our project life-cycle:

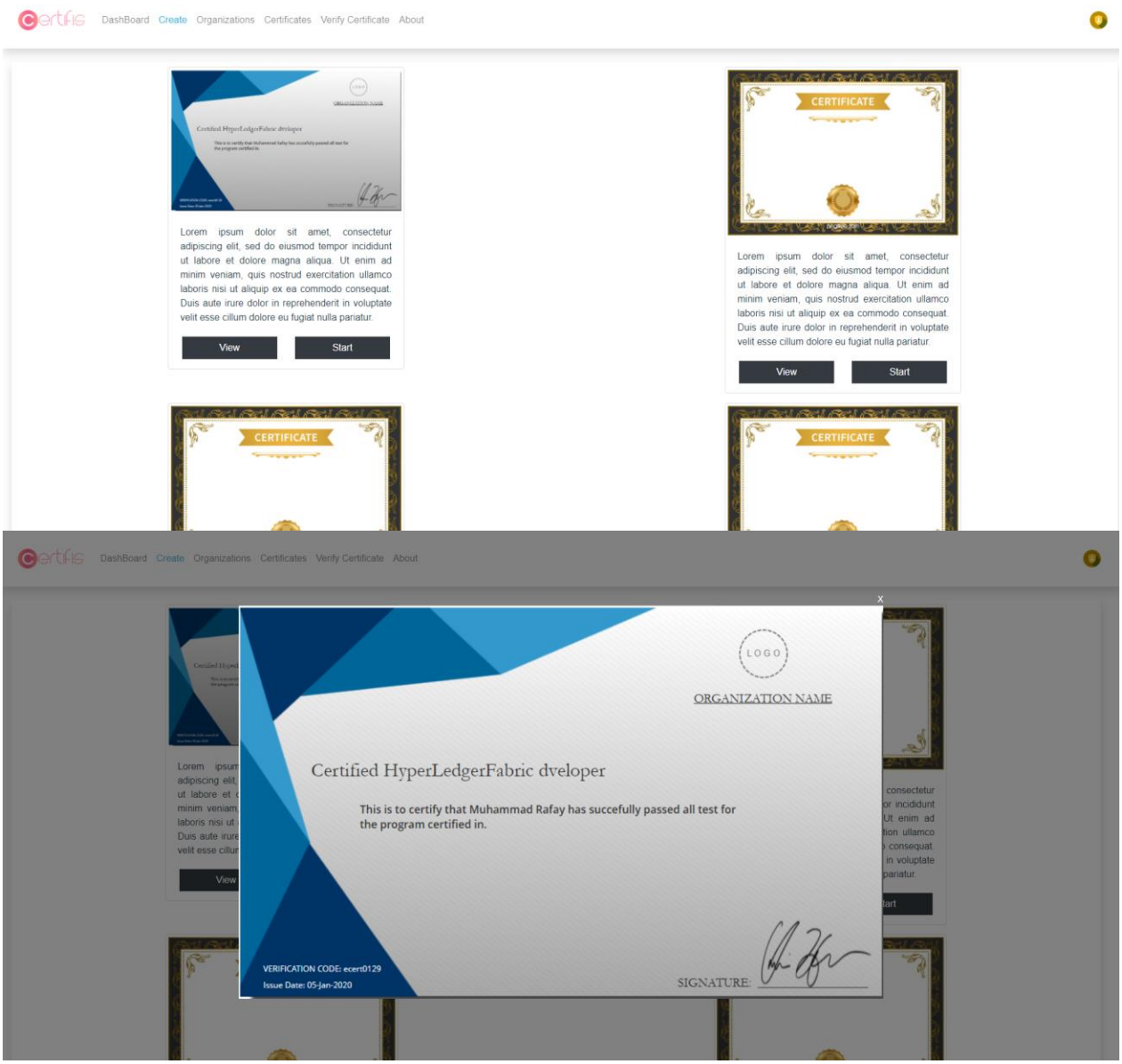
- Start developing wireframes as the part of requirement collection.
- Convert mockups to the actual UI.
- Web services will develop in parallel with UI implementation.
- Web services will continuously be integrated with front-end apps.

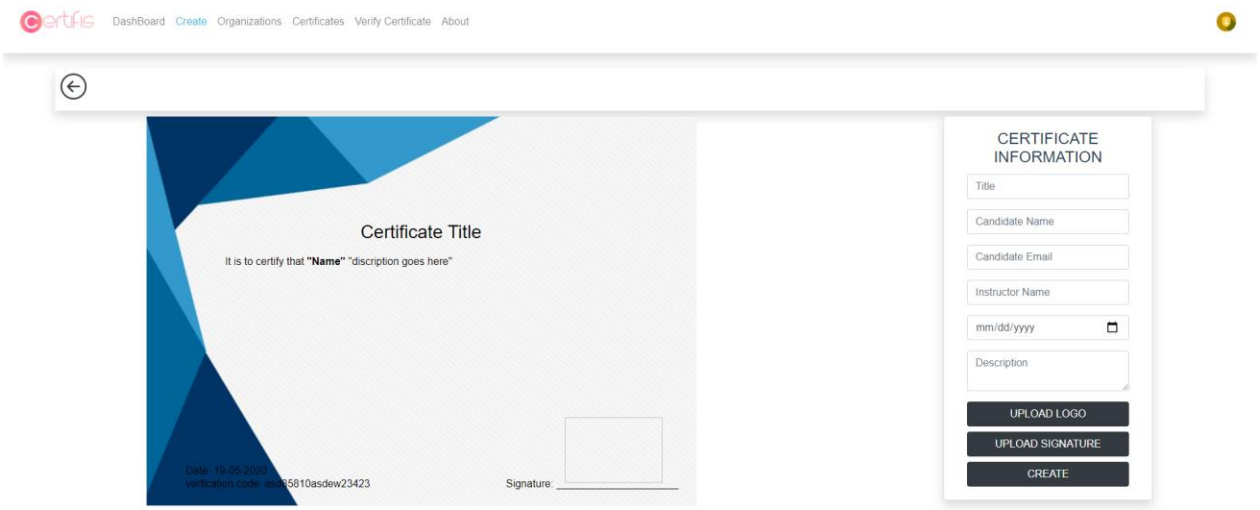
- Deploy the complete web app with a local database and test the complete functionality of the app without blockchain integration.
- Now we will start blockchain development.
- Writing & deploying chain-code on sample network.
- Test the working of chain-code.
- Developing & integrating the blockchain services with the web application.
- Integrate the publishing and querying blockchain web services with client apps.
- Now test the working of the system as whole with the blockchain (sample network).
- Design a fully custom block chain network according to business requirements.
    - Writing configs for blockchain (a config automation engine will have been developing in parallel with the development of config files).
    - Developing bash scripts for deployments.
- Install the chain-code on the newly designed network & test it again on the local host.
- Now prepare for deploying a production ready network so first we will deploy it in our multi host network environment. Multi-host deployments may require changes in scripts on multi host environments.
- Write the blockchain connection profiles and integrate it with the actual system and now test the complete multi host network.
- Now for scalability purposes we will develop scripts to add new peers in current organizations in the production environment.
- Write scripts to setup and add new organization to the current channel in production environments.
- Writing scripts to update the chain-code.
- Writing script to endorse or validate the proposal of installing or updating chain-code.

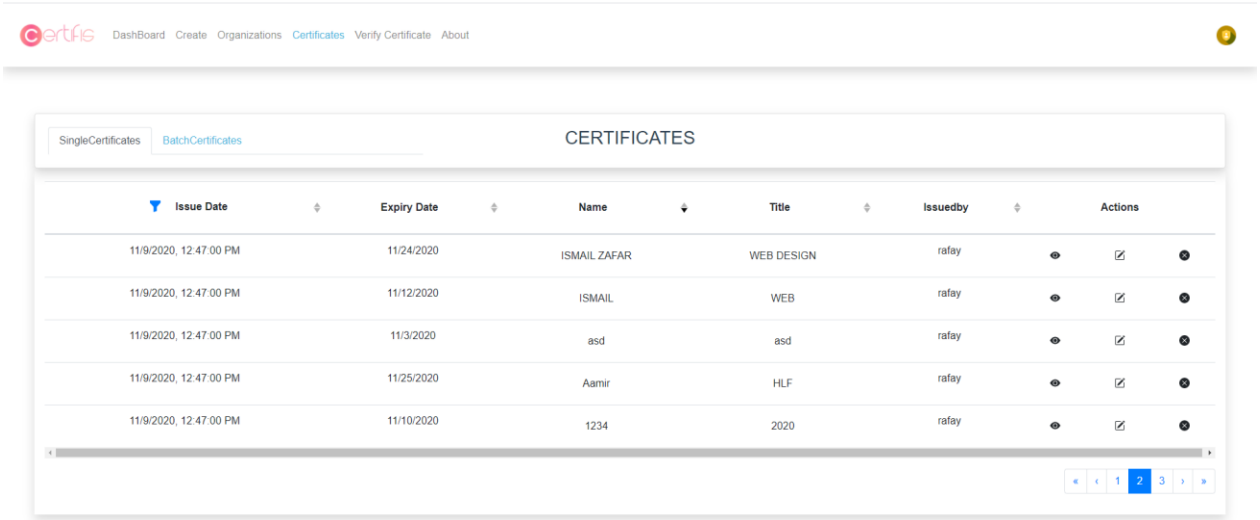
Tools and Technologies

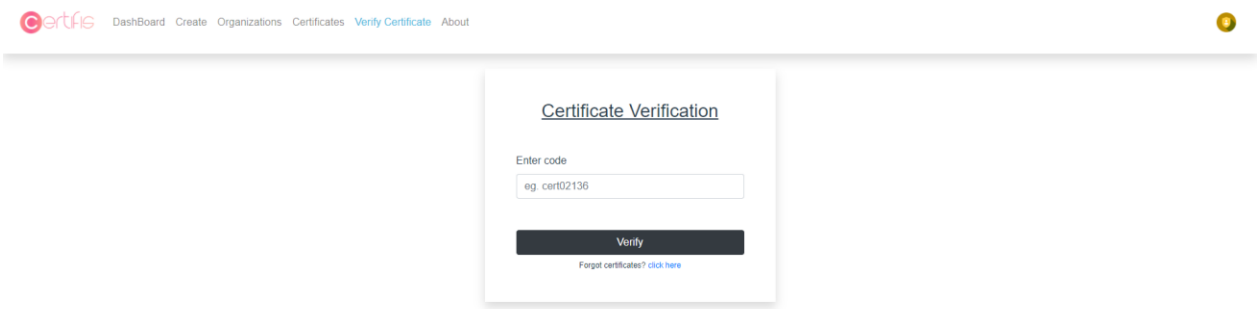
Operating System: Linux (ubuntu)
Language: Bash, js, html, css, yaml, json
Runtime: nodejs
Code Editor: VSCode
Back-End Frameworks: Express Js
Database: MYSQL/MONGODB
Front-End-FrameWork: vuejs
Block-Chain Framework: Hyperledger Fabric
Deployment: Docker, Docker-Compose

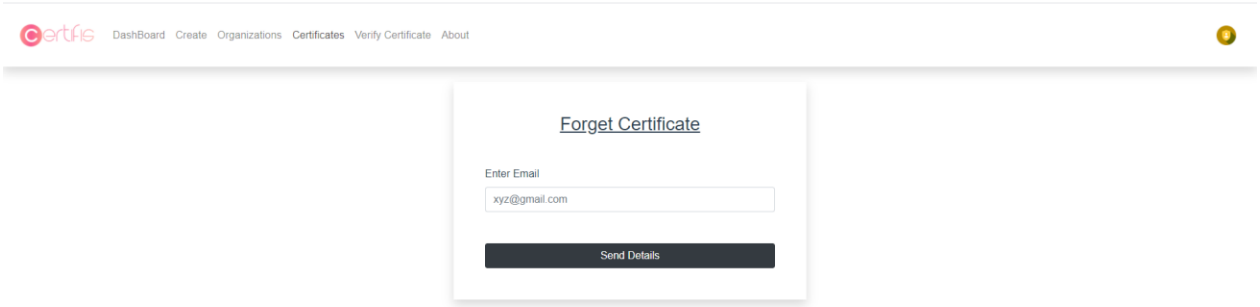
Expected Final product



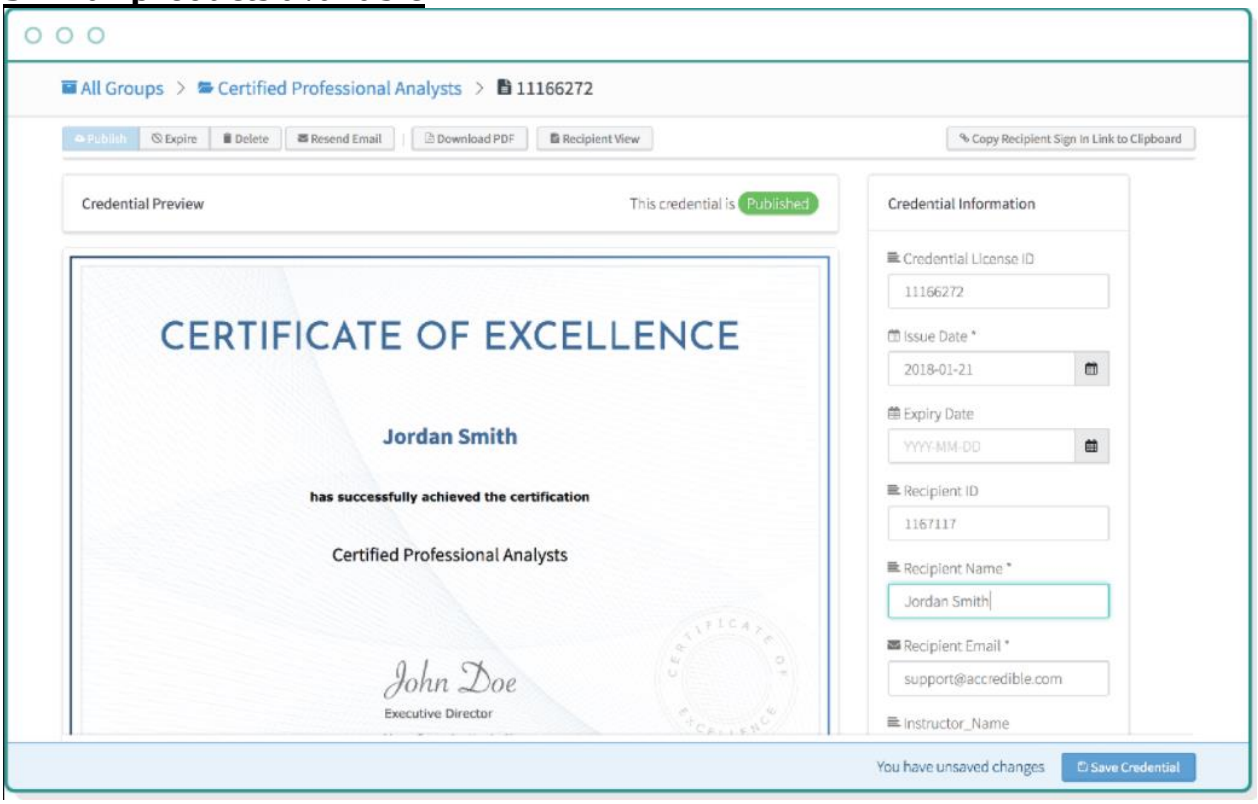

DashBoard Create Organizations Certificates Verify Certificate About
Certificate Title
It is to certify that "Name" "discription goes here"
Signature:
CERTIFICATE INFORMATION
Title
Candidate Name
Candidate Email
Instructor Name
mm/dd/yyyy
Description
UPLOAD LOGO
UPLOAD SIGNATURE
CREATE

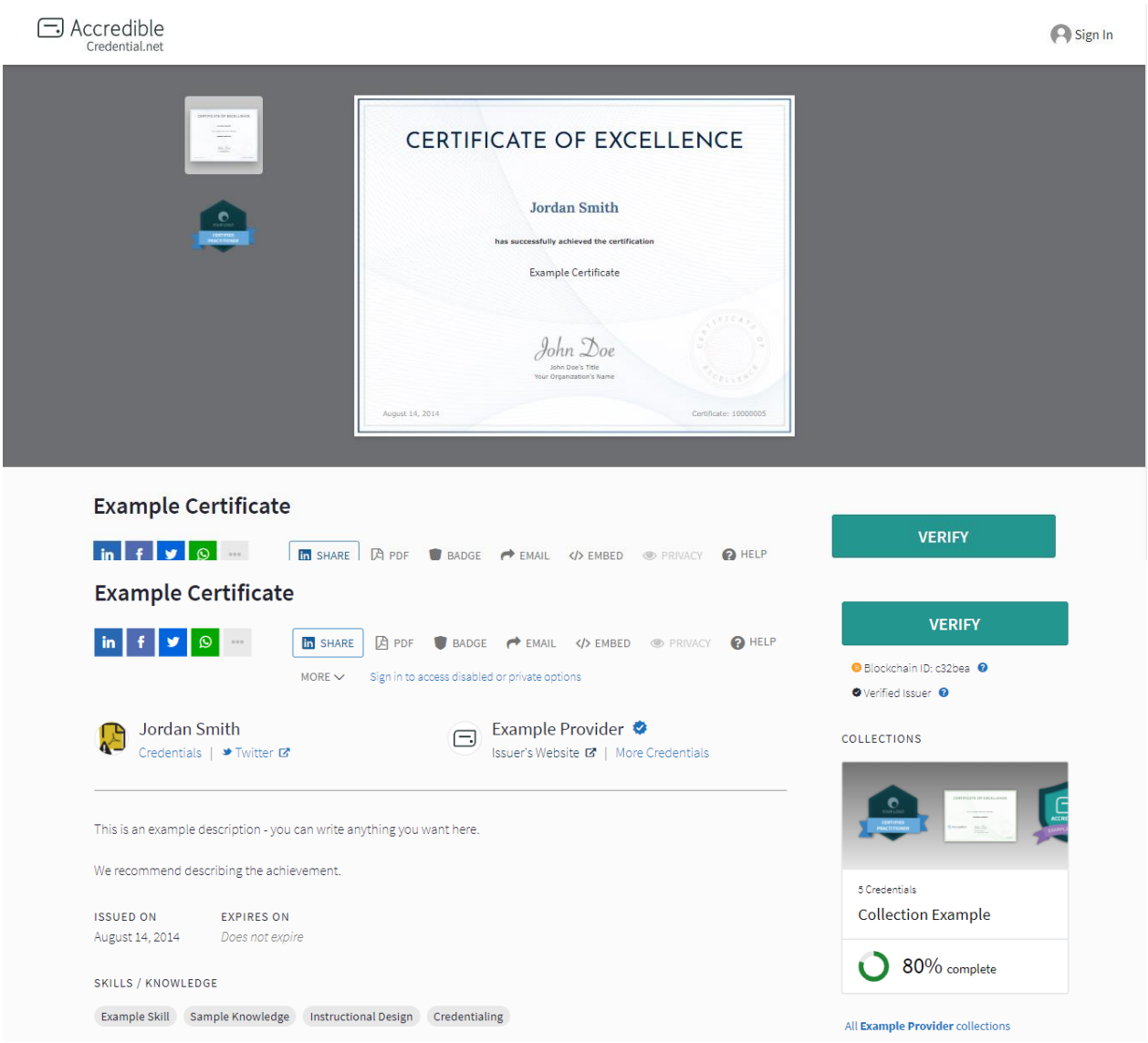

DashBoard Create Organizations Certificates Verify Certificate About
SingleCertificates
BatchCertificates
CERTIFICATES
Issue Date
Expiry Date
Name
Title
Issuedby
Actions
11/9/2020, 12:47:00 PM 11/24/2020 ISMAIL ZAFAR WEB DESIGN rafay
11/9/2020, 12:47:00 PM 11/12/2020 ISMAIL WEB rafay
11/9/2020, 12:47:00 PM 11/3/2020 asd asd rafay
11/9/2020, 12:47:00 PM 11/25/2020 Aamir HLF rafay
11/9/2020, 12:47:00 PM 11/10/2020 1234 2020 rafay
1 2 3

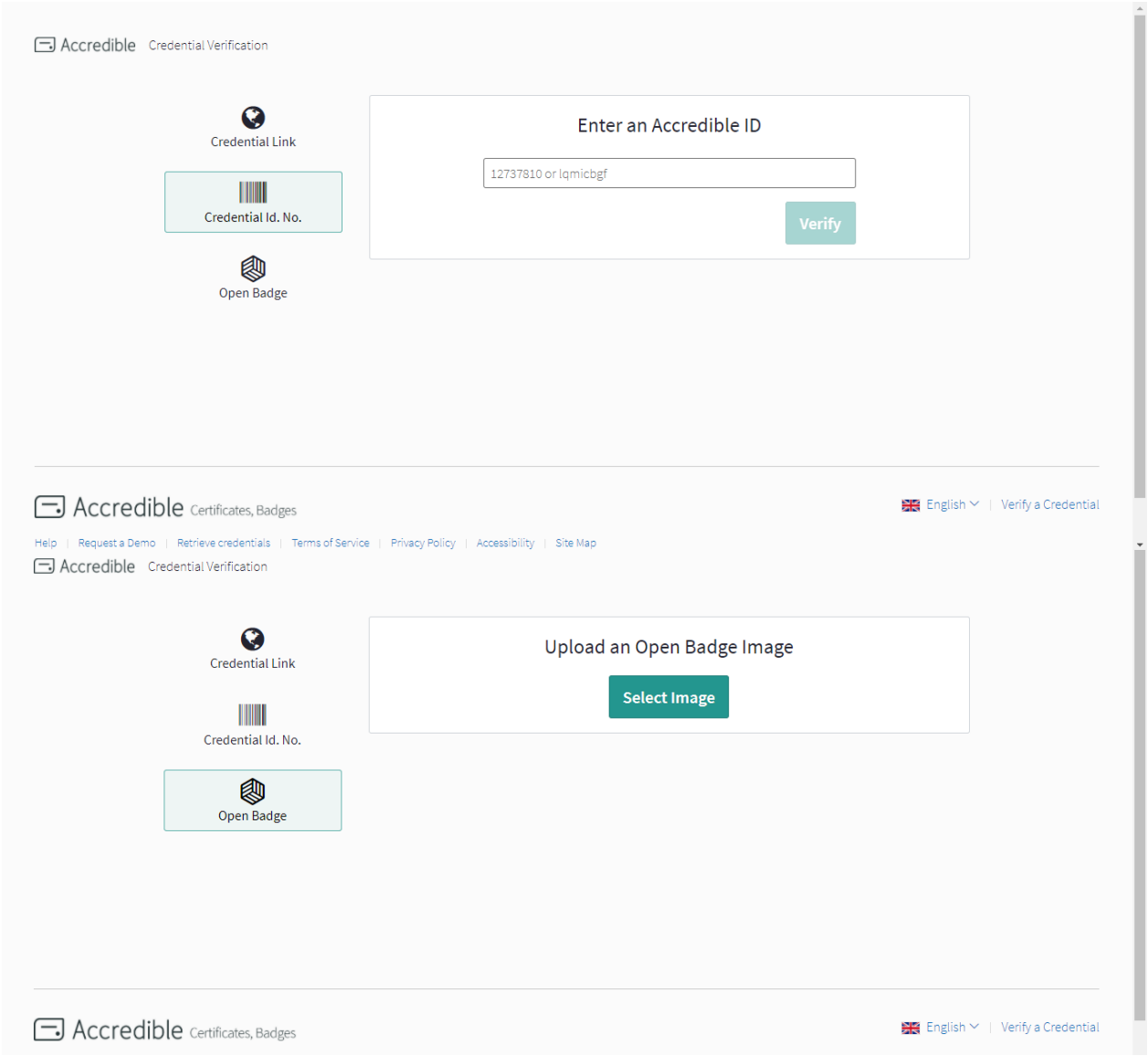

DashBoard
Create
Organizations
Certificates
Verify Certificate
About
Certificate Verification
Enter code
eg. cert02136
Verify
Forgot certificates? click here

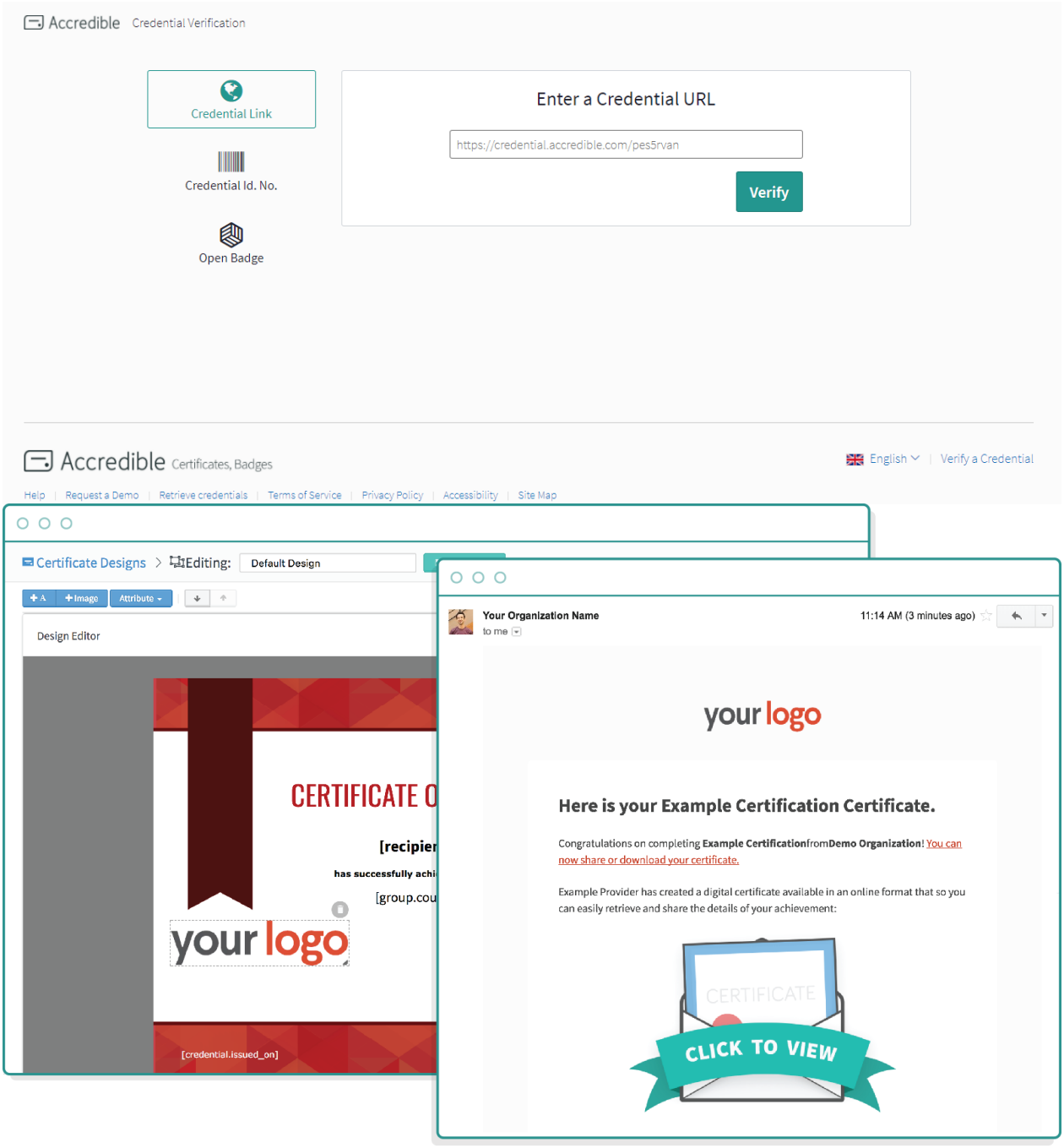

DashBoard
Create
Organizations
Certificates
Verify Certificate
About
Forget Certificate
Enter Email
xyz@gmail.com
Send Details

Similar products available




Accredible
Credential.net
Sign In
CERTIFICATE OF EXCELLENCE
Jordan Smith
has successfully achieved the certification
Example Certificate
John Doe
John Doe's Title
Your Organization's Name
August 14, 2014
Certificate: 10000005
Example Certificate
SHARE
PDF
BADGE
EMAIL
EMBED
PRIVACY
HELP
VERIFY
Example Certificate
SHARE
PDF
BADGE
EMAIL
EMBED
PRIVACY
HELP
MORE
Sign in to access disabled or private options
VERIFY
Blockchain ID: c32bea
Verified Issuer
Jordan Smith
Credentials | Twitter
Example Provider
Issuer's Website | More Credentials
COLLECTIONS
This is an example description - you can write anything you want here.
We recommend describing the achievement.
ISSUED ON
August 14, 2014
EXPIRES ON
Does not expire
SKILLS / KNOWLEDGE
Example Skill
Sample Knowledge
Instructional Design
Credentialing
5 Credentials
Collection Example
80% complete
All Example Provider collections


Accredible Credential Verification
Credential Link
Credential Id. No.
Open Badge
Enter an Accredible ID
12737810 or lqmicbgf
Verify
Accredible Certificates, Badges
English | Verify a Credential
Help | Request a Demo | Retrieve credentials | Terms of Service | Privacy Policy | Accessibility | Site Map
Accredible Credential Verification
Credential Link
Credential Id. No.
Open Badge
Upload an Open Badge Image
Select Image
Accredible Certificates, Badges
English | Verify a Credential



List down similar products available online with URL

https://www.accredible.com/

Project approvals:

Name: Dr. Muhammad Qasim Pasta
Project Supervisor Signature

Member, FYP Committee, UIT Signature