CS61065 Theory and Applications of Blockchain

Assignment: 5 : Hyperledger Indy

Date: 3rd November, 2022

Submission Deadline: November 13, 2022 EOD (Hard Deadline)

You can create a group of two and solve this assignment. Only one member from each group should submit the assignment in Moodle. Clearly mention your group details in the submission.

Sunil is a graduate of NIT Durgapur, who always wanted to pursue higher studies. Now, he wants to join the master's program at IIT Kharagpur. To support the finances, he went to apply for an educational loan from CitiBank. The bank requires the proof of an asset, and proof of admission to a reputed institute as evidence for the creditworthiness of the loan.
Sunil wants to use his existing house property, and student bonafide certificate from IIT Kharagpur for the loan.

In this assignment you need to implement a verifiable credential and verifiable presentation the flow using Hyperledger Indy, where there are 4 parties:

- Government
- IIT Kharagpur
- Sunil
- CitiBank

Government and IIT Kharagpur will be issuing the credentials for proof of property, and student certificate respectively to Sunil. Sunil will present the credentials to CitiBank that will validate his claims.

Submission Instructions

Create a directory and name it as A6_ROLLNUMBER. You need to create a single file which will execute the entire flow, and place it inside this directory. If you are implementing it in python, then name the file as **main.py.** Similarly for nodejs, name it as **main.js,** and so on. In the first line of the file, write your roll number as a comment. Compress the folder as a zip (with .zip extension). Upload the compressed file in moodle. Make sure you DO NOT include node_modules or similar library dependency files in your zip.

Part A:

1. Launch Indy pool by starting the docker image `ghoshbishakh/indy_pool`
   You may also choose to run it from the indy_pool repository.

2. Connect to the indy pool.
3. Configure one steward.
4. Register Verinyms for Trust Anchors - Government, and IIT Kharagpur

Part B:
Setup the credential schemas and credential definitions for PropertyDetails, and BonafideStudent. The government creates both the schemas in the indy ledger.
IIT Kharagpur registers a credential definition for BonafideStudent, and the Government registers a credential definition for PropertyDetails.
The schema for PropertyDetails and BonafideStudent are as follows:

```
{
   'name': 'PropertyDetails',
   'version': '1.2',
             'attributes':     ['owner_first_name',     'owner_last_name',
'address_of_property', 'owner_since_year', 'property_value_estimate']
}
```

```
{
   'name': 'BonafideStudent',
   'version': '1.2',
          'attributes':    ['student_first_name',    'student_last_name',
'degree_name', 'student_since_year', 'cgpa']
}
```

Part C:
Once the schema and credential definition setup is done, the issuers issue credentials to Sunil.

1. Government issues 'PropertyDetails' credential.
2. IIT Kharagpur issues 'BonafideStudent' credential.
3. Sunil saves both credentials to his wallet.

Use the following claims to create the verifiable credentials:

First Name: “Sunil”
Last Name: “Dey”

Address of Property: “M G Road, Chennai”
Estimated Value of Property: 1000000
Owner Since: 2005

Degree Name: “Mtech”
Student Since: 2022
CGPA: 8

Part D:
CitiBank requests a “loan_application_proof_request”, where the proofs for the following are required:

- first_name
- last_name
- degree_name
- student_since_year **[> 2021]**
- cgpa **[> 7]**
- address_of_property
- property_value_estimate **[> 400000]**
- owner_since_year

The claims in red must be from a credential issued by IIT Kharagpur.
Claims in blue must be from a credential issued by the Government.
For student_since_year, cgpa, and property_value, the values are not requested, instead the zero knowledge proof is requested to validate them (use 'requested_predicates’ for it).