ONE PERSON, ONE IDENTITY

With more than three billion internet users, each with multiple digital identities, the management of these identities is very important. Surveys show that people often use the identity management systems they don't want to use. They don't have full control over their infor mation, have no way to know what is shared with other parties and are dependent on trusted parties when logging in to websites.

Some of the Problems with the current Identity Management system which will be solved by this project.

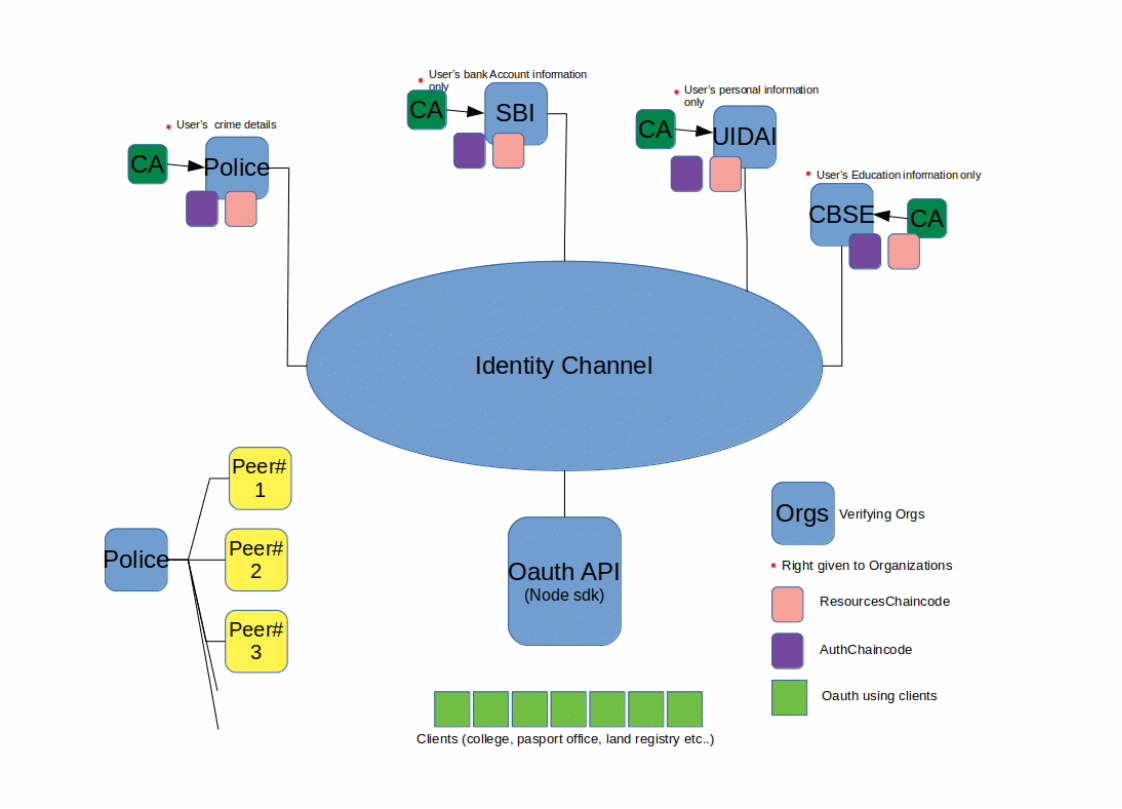
1. Single authority has the ultimate power to verify, revoke , edit any identity . This single point authority itself destroyed the actual definition of identity.
2. There is a single point of failure.
3. Users have to repeat the same KYC process across applications
4. There is no OAuth system for clients like (colleges , insurance , telecom companies ,passport office, etc) to verify any identity.

What is different about this project?

Yes , we know there are many projects which are leveraging blockchain for identity management. But most of those projects don’t integrate itself with the current system which creates problem of scalability and acceptability for these projects.

Implementation

Network Architecture



Network component

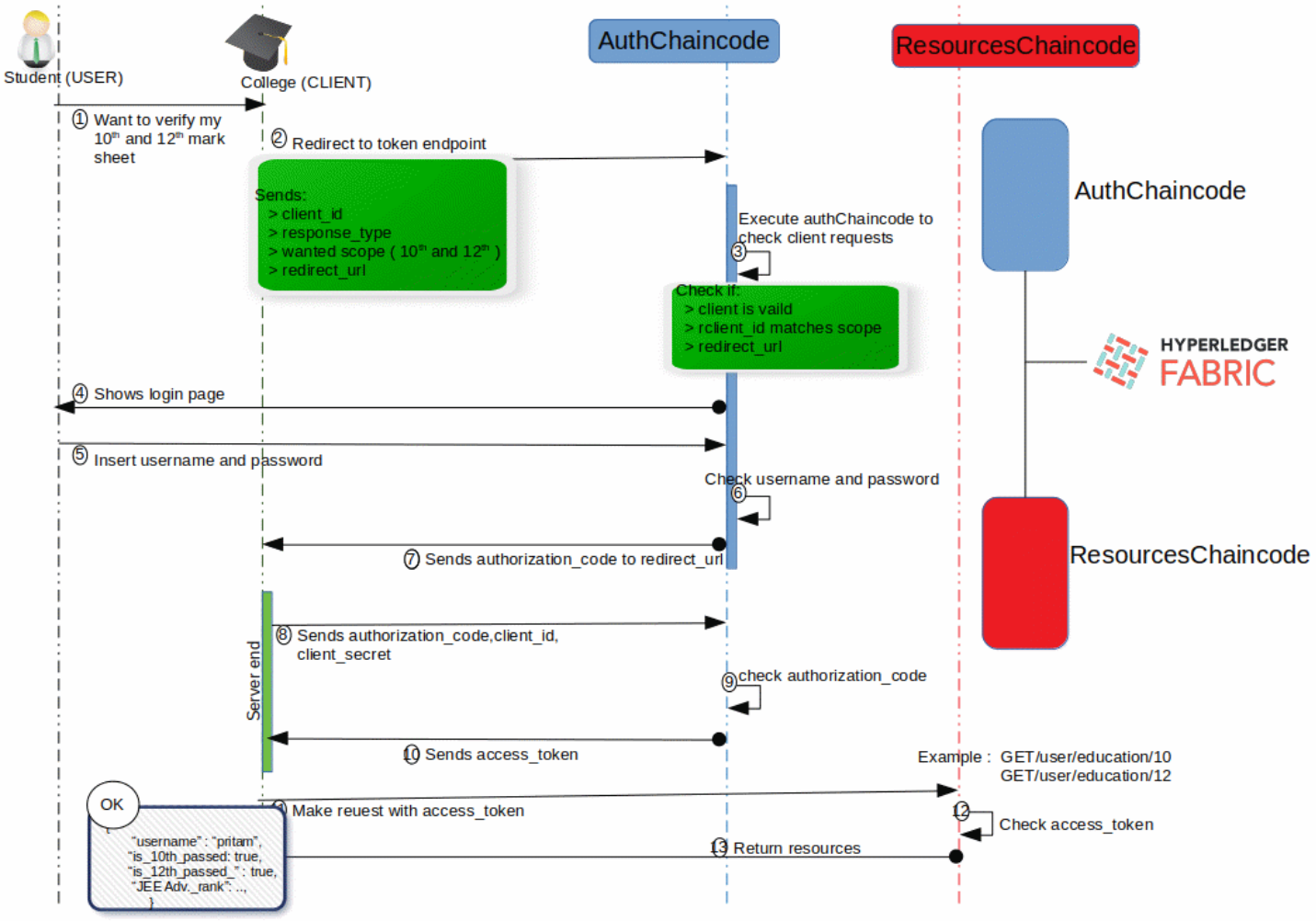
Identity channel : All organization will use this channel for identity creation,maagment, and verification.

Orgs: various organizations will be responsible for updating the field of the user's identity. The organization can only update those fields of user's identity to which it is authorized to update.
For eg. CBSE orgs can only update fields related to education details of any identity likewise Police can update only crime details field of user's identity.

CA: each orgs will be having Certification authority for registering and enrolling new peers to the Org

Peers: Each org will have hundreds of peer (node) spreading over country, each peer will be under a single orgs. These peers will act as local offices in cities, towns.

OAuth System (similar to Oauth 2)



Aouth component

ResourceChaincode: will manage the user's identity. In the OAuth system, the resources will be provided by this chaincode.

AuthChaincode: will manage authorized client's details, who can use the identity OAuth system. If the client is from the educational background then the client will be verified and registered by CBSE orgs only.

At last, the API will be hosted on central government servers, for security purposes.

Practical Use case examples:

- While making the passport user would not have to go to the police station, Passport client can simply check all the details for the criminal activity of the user using the Oauth system.

Technology stack to be used for the project

- Golang (for writting chaincode)

- Docker or kubernetes (to setup the peers,CAs,Orderes)

- Node.js (for OAuth API using express framwork)

- javascript, HTML , CSS (front-end)

- Cryptography (to secure the identity)