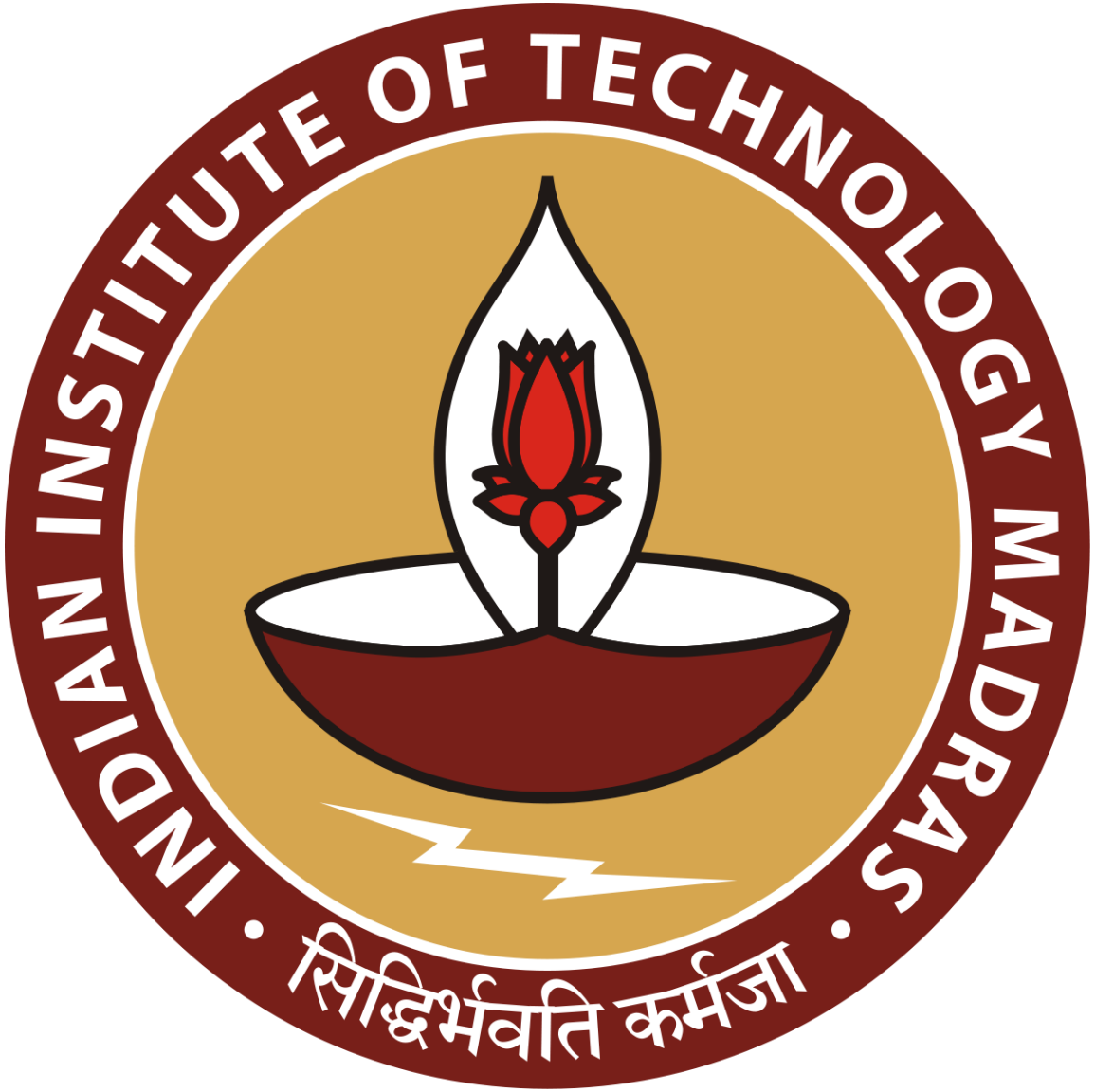


B. Tech Project- Blockchains in Business Networks

YADUGIRI SAIKUMAR, EE14B067, UNDERGRADUATE, EE DEPARTMENT, IITM

GUIDE: DR. SHWETA AGRAWAL, ASSISTANT PROFESSOR, CSE DEPARTMENT, IITM

CO-GUIDE: DR. KRISHNA JAGANNATHAN, ASSISTANT PROFESSOR, EE DEPARTMENT, IITM

Contents

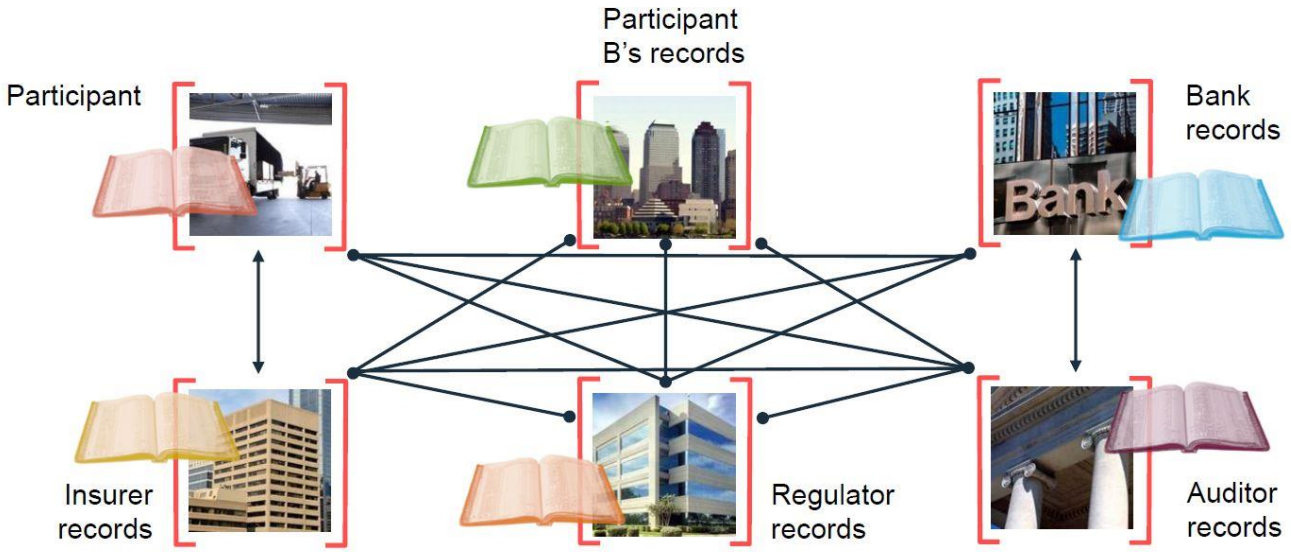
Problem

In any business network, between two organisations or among several organisations or even in a single organisation, trust is a key element.

A ledger is the key in any business to maintain a record of all the transactions that have occurred and constantly maintain the updated values of all the assets and also show accountability.

The notion of a non-uniform ledger when regarding a business network in which millions of transactions take place per second is ruled out as it is slow and can be easily corrupted.

- A single error in any of the ledgers can create a loss of trust among the participants.
- It is highly space consuming and computationally highly exhaustive.



… inefficient, expensive, vulnerable

Blockchains are trusted, distributed ledger systems which provide consensus, provenance and immutability.

As the name suggests, it is a chain of blocks with each block depending on the previous chain present.

These were invented for the cryptocurrency Bitcoin as its public transactional ledger system.

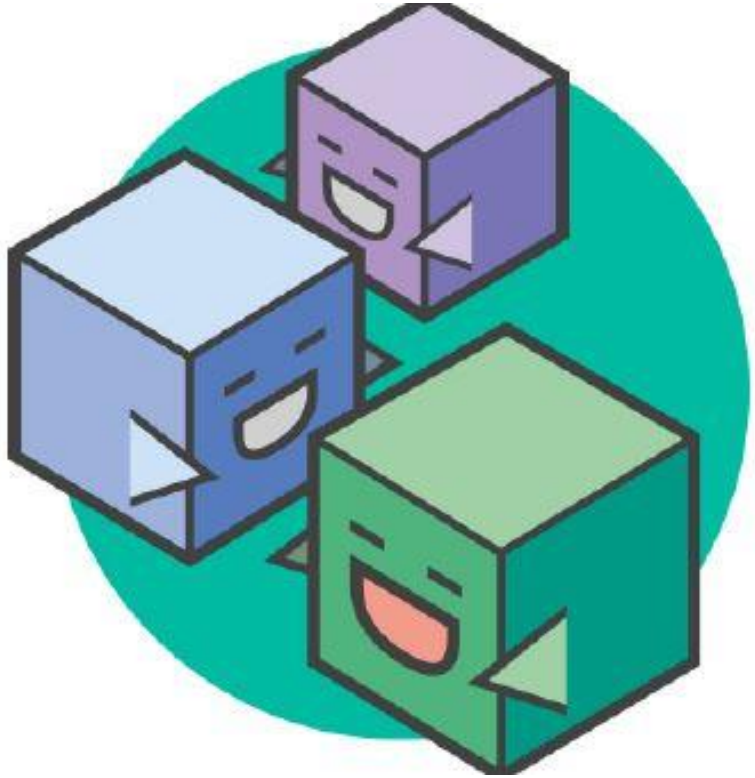
They also can be used as smart contract system which provide constraints for a transaction.

Solution - Blockchains

Blockchains for Business

- By using blockchains for business networks, we have the advantage of–

1. Shared Ledger : An append-only distributed system of record keeping uniform among all participants of the network.
2. Smart Contracts : We can include the terms of transactions in the business network and execute only if the conditions are met.
3. Trust: As the participants endorse the transactions, assets in the business network can have a verifiable audit trial.
4. Privacy: …



Different types of Blockchains – Permissioned Blockchains

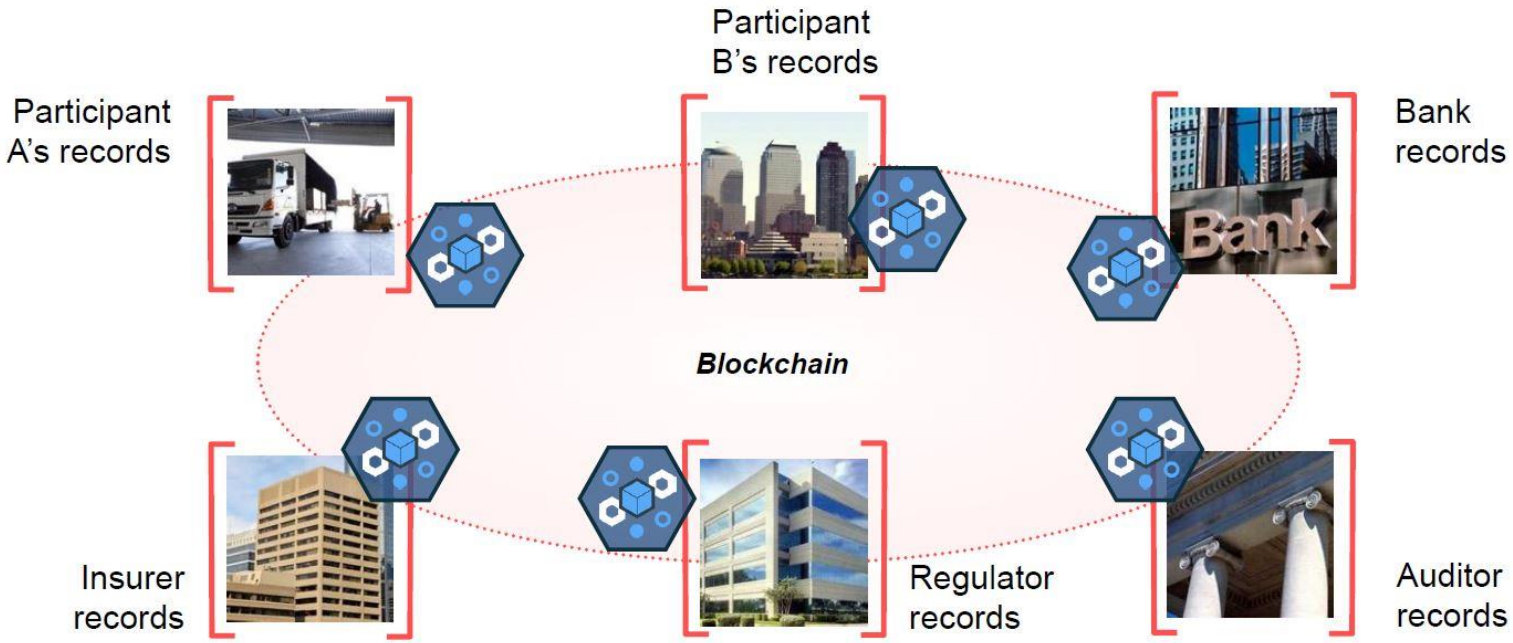
We are interested in Permissioned blockchains as public blockchains reveal too much and private blockchains withhold everything.

In a permissioned blockchain also known as a consortium or federated blockchain, a group of people decide the entry and exit into a network and privileges of the participants of the network.

It is computationally resourceful to use permissioned blockchains.

The main difference between among public, private and permissioned blockchains is in the genesis or the first block in the chain. It consists of a certificate which can be changed by the members.

- By using blockchains, we save space, computational power and increase trust.
- As blockchains are secure by design, they provide consensus, immutability, provenance and finality.
- All the aspects desirable in a business network.

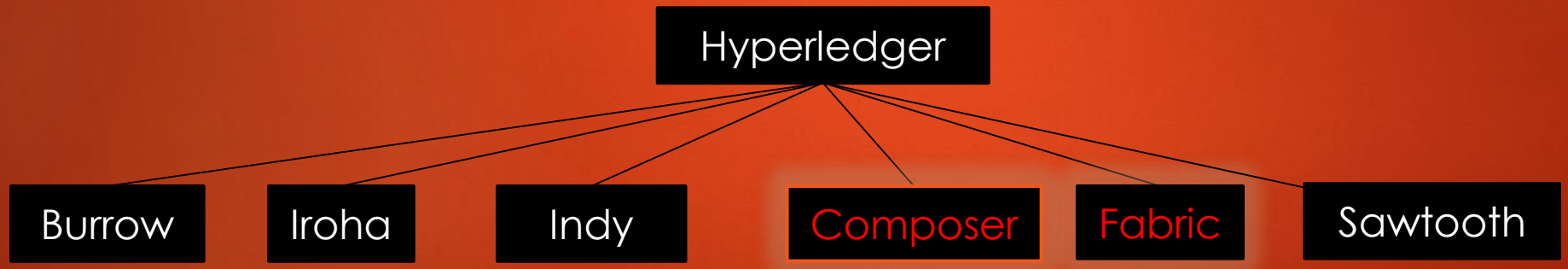


Summary of Blockchains

- Use of blockchains provide

Project Details

- Building business networks using blockchains is the main goal of the project.
- Experimented with different open source blockchain technologies like MultiChain, Hyperledger etc.



Hyperledger is an open-source umbrella project developed through the combined efforts of The Linux Foundation Group and IBM. It is used to advance the usage of blockchains in Internet of Things, Banking and Finance sectors.

Hyperledger is itself a suite of more than six different projects and we focused majorly on Hyperledger Fabric and Hyperledger Composer.

Developed two business networks using Hyperledger composer and the corresponding Hyperledger Fabric version.

…continued

End Goal

The main goal of the project is to develop a ledger system which suits both commercial and public needs.

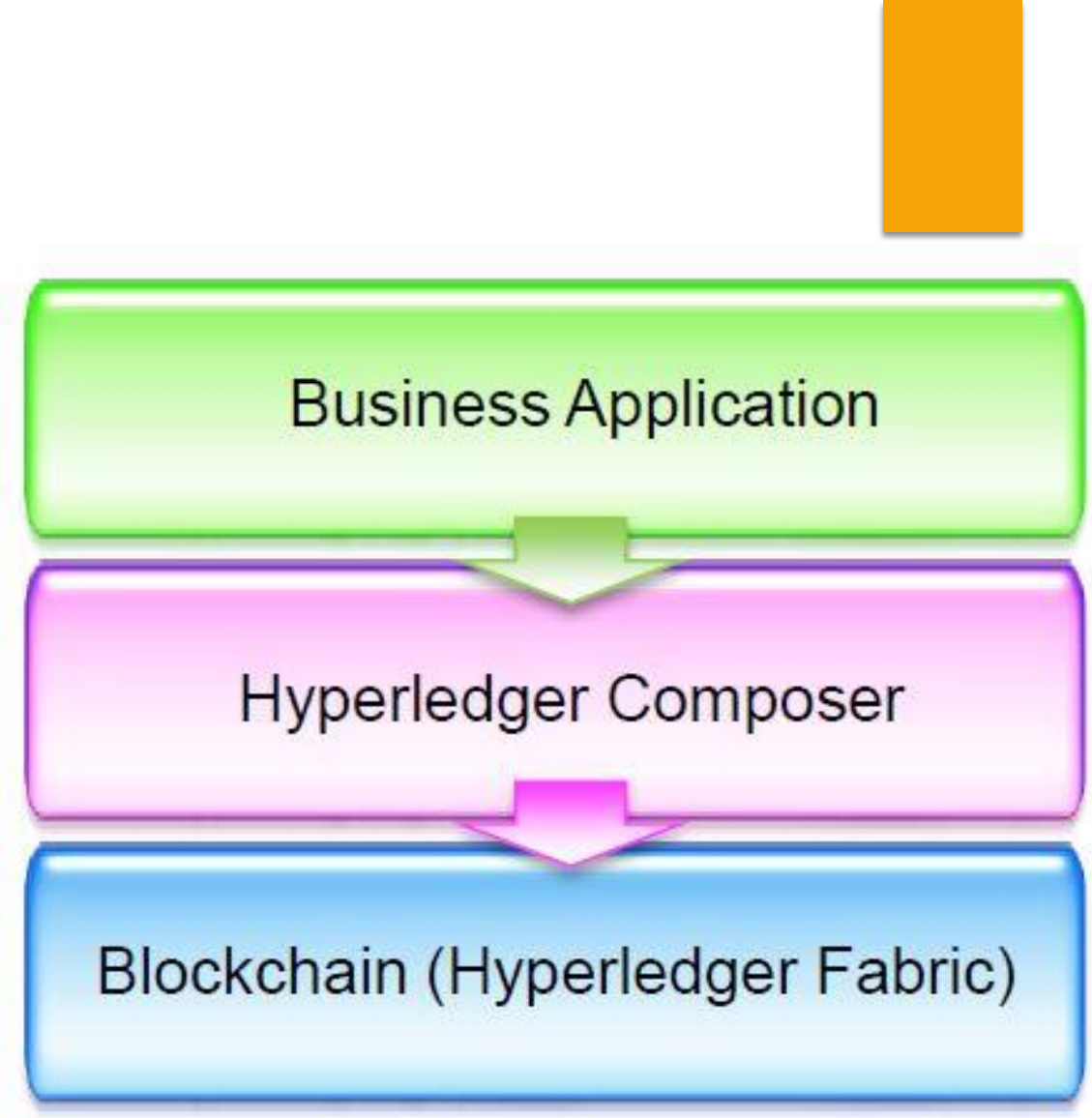
The project to develop and try out blockchain networks has already been approved by the Government of India.

Many other countries such as the Great Britain and Estonia have already started using blockchains as a shared ledger.

Some of the advantages to use this kind of blockchain network is that we can use it to store land records or Aadhar data etc.

Hyperledger Fabric

- This is suite used to build the bare essentials of the blockchain in the network.
- We can use this to optimise the blockchain performance required for our data.



Hyperledger Composer

Hyperledger composer provides a framework and toolkit to develop blockchain applications. This can be run both locally and in the cloud.

It supports the existing Hyperledger Fabric and provides pluggable blockchain consensus protocol so that the end user has simple and controlled access points.

One of the main advantages of using Composer is that it is free and open source with lots of documentation and support. It uses modern scripting languages, JavaScript.

Working of Hyperledger Composer

As the name itself suggests, we compose the ledger and it is here, we take advantage of the permissioned blockchain setting.

The basic components of hyperledger composer include

- Participant
- Asset
- Transaction

All these can be modelled in a .cto file and the logic for the transactions can be written in a separate JavaScript file.

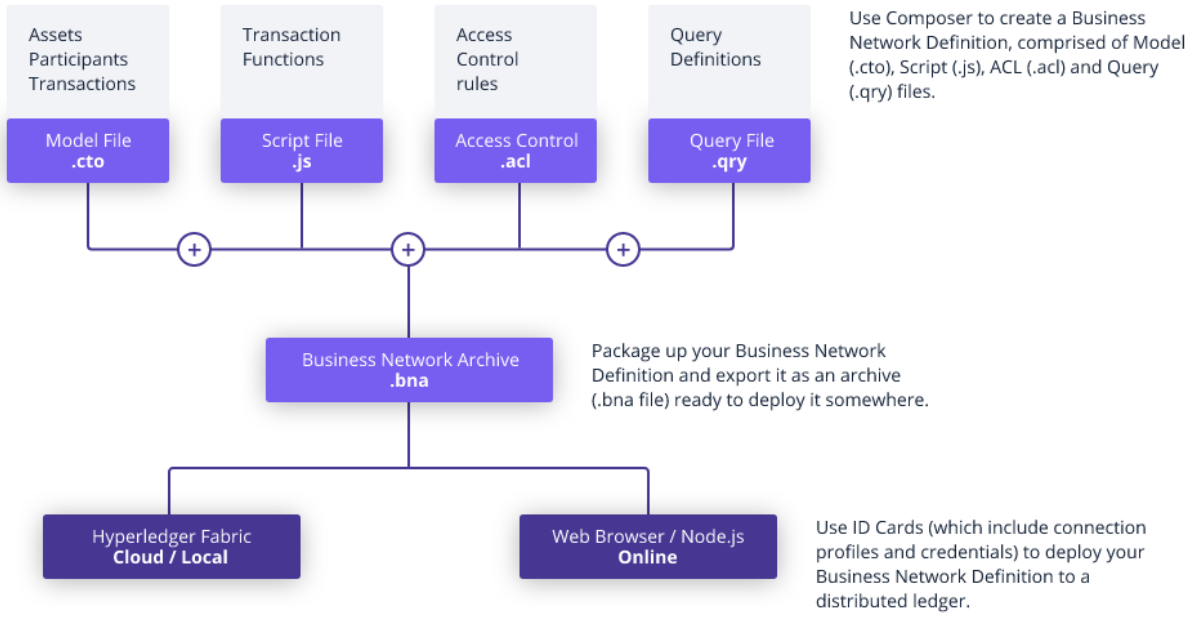
Access Control and Queries in Hyperledger Composer

In a permissioned blockchain setting a group of people have control over who does what and who can see what.

This is specified using a .acl file in the composer architecture.

Queries are also a useful thing in composer where one can perform a variety of queries using the same sql language. But the main difference is that it is done on a blockchain rather than on RDBMS.

Bird's eye view of Hyperledger Composer



System Requirements to work with Hyperledger Composer

Recommended System Configuration	My System Configuration
OS: Ubuntu 16.04/14.04 LTS, 64-bit	OS: Ubuntu 16.04 LTS, 64-bit
Docker Engine version 17.03 or higher	Docker Engine version 18.03
Docker-compose version 1.8 or higher	Docker-compose version 1.13
Node version 8.9 or higher	Node version 8.10(node 9 isn't supported)
npm version 5.x	npm version 5.7.1
Git version 2.9.x or higher	Git version 2.17
Python version 2.7x	Python version 2.7.12
VSCode Editor	Sublime 3.0 build 3143

Project with Hyperledger Composer

Some problems faced

The data size was too much for my local system. If we can have a designated server to host, this can be easily solved.

As the data grows, the time taken for the block to be added also grows as the peers would take time to respond. This is also an unsolved problem known as the Bitcoin scalability problem concerning the ledger system, blockchains, used in Bitcoin network.

Further possible developments

- Bring in real world data.
- Optimise blockchain structure for maximum performance.
- Integration of the two working networks and adding interactions between them.
- Use of BigChainDB to hold the data for blockchain.
- Improving the existing websites with more features such as one button queries etc.
- Asynchronous updates for pages.

References

Official Hyperledger website - https://hyperledger.github.io/composer/latest/

API documentation – https://hyperledger.github.io/composer/unstable/jsdoc/

YouTube channel – Zach Gollwitzer - https://www.youtube.com/channel/UCDwlw3MiPJXu5SavbZ3_a2A

Course on Blockchain development by IBM - https://www.coursera.org/learn/ibm-blockchain-essentials-for-developers

CS6530 – Applied Cryptography JAN-MAY 2017 by Dr Chester Rebeiro, IITM.

CS6111 – Foundations of Cryptography JUL-NOV 2017 by Dr Shweta Agrawal, IITM.

Thank you

YADUGIRI SAIKUMAR, EE14B067, UNDERGRADUATE, EE DEPARTMENT,
IIT MADRAS