1. If you have to create an application to automatically detect whether metamask is installed? Application which runs on your chrome browser which will detect metamask is there or not?

Answer -:

web3.currentProvider.isMetaMask === true.

function onLoad() {

if (typeof web3 !== 'undefined') {

// Use Mist/MetaMask's provider

web3js = new Web3(web3.currentProvider);

console.log("Using Metamask/Mist WEB3 provider")

} else {

alert('MetaMask not loaded ?!?')

return

}

}

2. What’s the purpose of Fabri-CA (certification authority) in hyperledger fabric? How it works. How the flow happens?

Answer -:

<https://medium.com/swlh/hyperledger-chapter-10-blockchain-application-on-hyperledger-fabric-2e34f3f430b>

Once the network is up. Let’s register Admin.

node registerAdmin.js

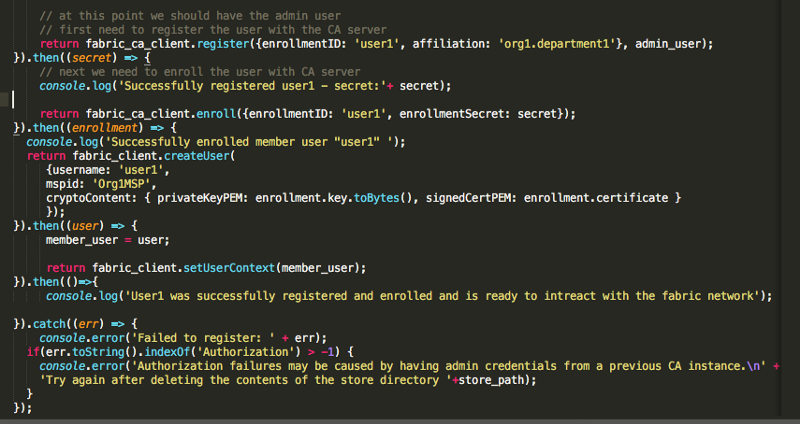
You should get this output, basically an Admin is created with the required keys.



Basically, withe the Fabric CA client we check if an Admin is already registered, if not it enrolls with the CA client. Basic parameters such as enrollmentID, Secret are set. Then the user is created with FabricClient with membership ID, along with the public private key pair.

Now that the network and admin are set, let’s register an User.

register user with the CA server and then enroll.



3. How transaction in Hyperledger fabric actually flows? What’s the flow sequence of transaction in Hyperledger fabric network.

Done

4. Suppose i want to create a chaincode and from chaincode i want to call an external service to get external database information. How to do it?

Answer -:

<https://hyperledger.github.io/composer/v0.19/integrating/call-out>

The request module (<https://github.com/request/request>), is a popular HTTP client used by many Node.js applications. Hyperledger Composer embeds the request module, so that transaction processor functions can use it to make calls to HTTP or REST APIs.

<https://lists.hyperledger.org/g/fabric/topic/17550096>

One way around this issue is to use a distributed external API with versioned data such that all endorsers store the external data's current version in the asset repository in world state as well.

This makes certain that the data read is identical and accounts for delays in propagation in the network.

Why Smart Contracts in Blockchain Need to Avoid Non-Deterministic Functions

<https://dzone.com/articles/why-smart-contracts-in-blockchain-needs-to-avoid-n>

Non-deterministic functions used in smart contracts have the potential to make the smart contracts totally useless.

All operations on the Blockchain should be deterministic. Simply put, the same operation performed across different nodes should return the same result. A difference in results between the nodes for the same operation can lead to a failure in consensus, since storing this data on the ledger will lead to an inconsistent ledger state thereby making the whole smart contract useless.

Determinism also refers to the fact that the same operation replayed on a different node at a different point in time should also produce the same results. For example, a new node that's been on-boarded to the network should be able to replay all the operations and end up in the correct ledger state, just like existing nodes.

The following are a few examples of non-deterministic operations on the Blockchain:

* Using a timestamp inside the smart contract and storing the timestamp on the ledger.
* Calling an external API (running outside the Blockchain) from the smart contract.

The optimal solution to capture a timestamp with milliseconds is to pass this information from the client application by invoking the Chaincode. Passing a timestamp as input to the smart contract will make sure that the same value is passed as the input to all the nodes executing the Chaincode, resulting in a deterministic operation.

12. What are the steps of taking the certificates from the certification authority? Where these certificates actually gets stored?

Answer -:

<https://openblockchain.readthedocs.io/en/latest/Setup/ca-setup/>

<https://blog.knoldus.com/hyperledger-fabric-certificate-authority/>

Fabric Certificate Authority (CA)

Fabric CA is a tool through which you can generate certificates.

Let say you have 10 users then, 10 certificates get generated for 10 users. You can add additional information called as attributes in certificates. So this information is propagated to the system.

Chaincodes ([Smart Contracts](https://blockgeeks.com/guides/smart-contracts/) in Blockchain) can read this data and perform different operations As this information is within certificates you can’t modify it which makes process secure.

You can generate certificates by specifying the username, password and affiliations which is called as **Enrollment**.

With these certificates you have to sign each and every request.

Fabric CA Architecture

Fabric-CA root Server is the root node of the entire tree.

You can interact with Fabric-CA Server via Fabric-CA Client or through one of the Fabric SDKs.

 There can be multiple Fabric-CA Intermediate Servers.

The client routes to an HA Proxy endpoint which load balances traffic to one of the fabric-ca-server cluster members.

All Hyperledger Fabric CA servers in a cluster share the same database for keeping track of identities and certificates.

19. I want to call the external service from the smart contract on your main network? how would i do that? This is for Ethereum

Answer -:

<https://medium.com/aigang-network/how-ethereum-contract-can-communicate-with-external-data-source-2e32616ea180>

Ethereum virtual state machine cannot communicate with the outside world in the simple and an easy way. Why?

Because to approve each block-chain BLOCK validity, **all mining nodes should get the same results from the outside**. And it is not an easy task to deal with that.

There are two ways how this can happen: Pull way or Push way.

Pull way:

To use this method you should trust 3rd party solution like [Oraclize](http://www.oraclize.it/). This service is not free and you should pay them

 No data security available here

Push way:

Listens what to update

You can control all process, no 3rd party components.

Need Custom development and hosting for “Custom Executor”.

20 & 21. Difference between fabric & Sawtooth? Coming to throughput which one is better.

Answer -:

<https://www.skcript.com/svr/should-i-choose-hyperledger-sawtooth-1-0-over-fabric-1-0/>

Hyperledger Sawtooth for example, focuses on creating very secure way to handle your smart contracts, with stricter rules and consensus.

[Hyperledger Fabric](https://www.skcript.com/svr/5-advantages-of-using-hyperledger-fabric-for-your-enterprise-blockchain/) on the other hand, can optionally enforce these rules, which helps a lot of different private blockchain providers right now.

Sawtooth 1.0 features -:

**Secure Smart Contracts;** With a strict policy to have your information truly distributed, the Smart Contracts are safer and Enterprise ready.  it comes with Byzantine Fault Tolerance features. This BFT feature gives much higher tolerance rate than the Crash Fault Tolerance in Fabric.

**Parallel Transactions;** The ability to have parallel transactions with Sawtooth makes all the difference. Thus reducing the amount of time it takes to process transactions in the system.

If you are looking at a private blockchain network that holds highly sensitive data and a sensitive smart contract, Sawtooth could be one option you should consider.