**Block-chain and Hyperledger: A Very Brief Guide**

*- Ish Handa*

**Introduction**

A “**Centralised**” **(Server/Client)** network means there is a sole entity which has access and control over the data and flow of information in the network. Currently, all our transactions are centralized implying that all our transactions are handled and processed by a trusted third-party institution. We expect them to make evaluative and reasonable decisions, yet this third-party institution is not completely reliable. Most transactions incur large time and money costs.

Thus, comes Blockchain technology which can achieve high transparency, accountability and safety, reduce costs and complexity as it is based on a distributednetwork. The distributed network is also a decentralized network meaning that no single party is in control of the flow of the data in the network.

**Distributed Ledger**

In accounting, a ledger is a book which is used for recording and totaling transactions.

Similarly, a distributed ledger is a digital ledger is a digitalized version of this accounting letter, where each participant in the network, owns an always updated copy of the ledger. This helps the Blockchain achieve the following

1. **Efficiency**: No central authority to control the flow. Since all participants in the network possess the same copy, only one transaction registration is required in complex interactions between multiple parties.

2. **Reduced cost:** As mentioned above, only one registration is required thus saving time and cost. Also, no intermediate parties are required to handle these transactions, further reducing costs.

3. **Secure, Temper-proof**: The ledger using the concept of consensus which means that all participants in the network must agree before making changes to the ledger. The ledger also using cryptic digital signature verification and hashing data structures to identify in-consistencies

4. **Transparency**: All transactions (with their respective timestamps) are accessible by all the participants.

**Consensus**

A consensus means the agreement of all the participants in the network to modify and update the distributed ledger in the network. Proof of Work, proof of stake, proof of time and so on are all popular approaches used by different Blockchain as consensus forming mechanisms.

**Smart Contract**

A contract is an agreement between two or more parties. A smart contract follows the same ideology involving the agreement to be assets. It is well practiced software engineering concept, which in Blockchain allows participants to make automatic transactions while satisfying certain business conditions.

**Hyperledger**

Hyperledger is an open-source Blockchain development project hosted by the Linux

Foundation. It aims at enhancing the cross-industrial development of Blockchain technology.

Hyperledger project is backed up by many big companies like IBM, Intel, American Express and so.

There are 5 frameworks and 3 tools, they are Sawtooth, Iroha, Fabric, Burrow and Indy and Cello, Composer and Explorer. Each of these frameworks and tools contribute to their own use in the development process of a block-chain network in different ways.

**Fabric**

Hyperledger Fabric is a Blockchain solution for managing business use cases and their repective transactions supported by a modular architecture delivering high degrees of confidentiality, resiliency, flexibility and scalability

**Modular Architecture**

Hyperledger Fabric has a modular architecture that supports some pluggable functions

like Membership Service Provider (MSP) and different consensus mechanisms, to be run

in the implementations. This gives more flexibility in designing the Blockchain

applications.

**Ledger Structure**

There are 2 components in the Fabric’s ledger: World State and the Blockchain.

WorldState: LevelDB and CouchDB are options of state database maintains the current state of all nodes in the network.

Blockchain: The base of the block chain are hash**-**linked chains, these chains

are irreversible, tamper-resistive and chronologically ordered. They are a list of past transactions that have taken place in the network. Each network constitutes a separate ledger where each peer owns a copy.

**Permissioned Networks**

Hyperledger Fabric uses the permissioned network so that each transaction can

be confidential and more protected. This means that there is a central authorization and authentication system that decides who is a peer in the fabric network and has access to it.

The membership enrolling mechanism is called **Membership Service Provider (MSP)**, it

outlines who can join the network and the amount of control they have over the network, and they also define who can issue and validate certificates. The modular architecture allows one network to be operated by one or multiple MSPs, allowing different mechanism and designs in the business rules of the network.

**Chaincode**

Chaincode in the Fabric represents the smart contract. It defines the model of the assets and business rules that administrate the entire network. It is a set of transactional functions written in GoLang. When a client sends the endorser a transaction request to run the chain-code, the endorser will initiate the transaction by retrieving key/ value data from the state database (world state). It will then send a copy of the proposal response to the client with the endorser’s signature attached to the response. The client then broadcasts the endorsement and transaction payload to the orderer for ordering-services.

**Composer**

Hyperledger Composer runs the fabrics infrastructure and provides an easy to use platform for the development of Blockchain applications. It is used to model, test and deploy the business network and make transactions with it. With the help of Composer, business network can be easily modelled and Blockchain solution can implemented quickly.

Composer provides us we two platforms, namely Playground and Development

Tools. The playground tool can be run on a cloud platform or one’s personal machine and is a fast way of testing your network. Whereas the development tools provide a set of command line functions which helps in building in building the Blockchain network.

**Solution Structure**

The Composer solution constitutes of Business Network Definitions packed and stored into a Business Network Archive (.bna) file. A BNA file comprises of the following

**Model** (.cto): Defines the assets, transactions and its participants.

**Access Control** (.acl): Defines the authority that the participants of the networks have.

Different participants in the network may be given different right to create, read, update

or delete element in the network.

**Script** (.js): Defines the transaction processor function that will implement to the business

network model. The function will be automatically run in the runtimes when the

transactions are submitted.

**Query** (.qry): It is an optional component in the Composer solution which performs queries on the networks data to retrieve the desired information from the Blockchain.