

BLOCKCHAIN APPLICATION USING HYPERLEDGER

Prof. Umarani Chellapandy
.Dhanush S R
Master of Computer Applications
In
Information Security Management Systems,
Jain (Deemed-to-be University), Bangalore, India

Abstract: In this project, the concepts of Hyperledger Fabric and Hyperledger Composer concepts have been used to produce an enterprise level blockchain application. The Hyperledger Fabric concept is used for developing applications or solutions with a linked architecture, Fabric allows components, like consensus and membership services, to be easy to be deployed. Hyperledger Fabric influences container technology for hosting smart contracts called “chain code” that comprise the application logic of the system. Whereas composer helps a developer to make and build business architecture to be easily deployed in a blockchain environment. So, in this project Hyperledger Fabric supports as a pluggable runtime and is used to be stored on a distributed ledger. In conclusion, a basic supply chain management system can be implemented with the help of composer and fabric a model with entities like manufacturer, distributor, retailer and the end customer, the chain code which defines the logic of the project shall be invoked and instantiated by moving the product from one entity to other by following the rules that has been defined by the network administrator who defines the privileges and permissions given to various entities

I. INTRODUCTION

Any typical business which involves multiple people from manufacturer to the end customer including lots of transactions by moving the asset from one entity to another involves a lot of business process and charges making it a lot costlier to the end consumer. So, the concept of permissioned blockchain on a distributed ledger shall help the manufacturer and customer to decide on a price that can be kept as a secret between them about the price that they are dealing with. So, in an enterprise grade blockchain architecture the smart contract shall be signed by various entities like banking sectors, financial advisors, other large-scale consumers in a business transaction to keep it completely legal and secure. Yes, this is possible because all the entities would agree upon the smart contract and ledge the transaction but still keeping the transaction details completely private that is only between the customer and manufacturer.

In this application a supply chain management system has been defined by the model having a network administrator can create certificates and add participants like customers, retailer, distributor and manufacturer to the blockchain application an asset can be created as well and all these transactions including system and product transactions would be logged.

The following are some of the important features of Hyperledger block-chain:

Peer nodes: Data that are entered into the block-chain contain hash values and these hash values are what connect the blocks in a chain and each is linked to another using the previous hash value of the former. So, data cannot be altered later, why it is called immutable ledger.

Channel: Channels are a logical architecture shaped by collection of peers. This allows a group of peers in creating a separate ledger of transactions.

The Hyperledger Fabric network is made from the peers owned and contributed by the different organizations that are members of the network. This network exists because organizations subsidize their individual resources to the collective network. Peers have an identity or a certificate assigned by a Membership Service Provider from its owning organization. Peers of different organizations can be on the same channel.

Membership Services Provider: The MSP is implemented as a Certificate Authority to manage certificates used to authenticate member identity and roles. No unknown identities can transact in the Hyperledger Fabric network. It manages user IDs and authenticates all participants on the network which enables Hyperledger Fabric as a Private and Permissioned network.

Ordering service: This basically authenticates all the endorsement peers and MSP and ledge the transaction which will be reflected in all the peers regarding the transaction.

II. SIGNIFICANCE

A. Role of this project

The aim of project described by this article is mainly educative and informative. So this is to make understand block-chain in a simple but also clear way by using simple terms, explanations and implementation. As result of this paper we expect a detail explanation of how permissioned block-chain with a particular focus on security and privacy. More details are given in the description section.

A. Background

Blockchain technology is an upcoming trend in the industry. There are different types of blockchain technologies in which, permissioned blockchain technology where it can be widely used for enterprise level industries to ensure privacy. I have never seen any article of this works in the real-world business processes. Hence this article described in this paper can help readers who are interested in permissioned blockchain technology used for business purposes.

III. DESCRIPTION

This article aims to detail on development of a block-chain sample that can be used in a local network to show all the operations that can be done on a block-chain and how those operations are performed. Those operations are for example mining blocks, make the block-chain decentralized, make transactions, make divers changes etc. The different modules included in this project are described below in details:

A. Initiating Hyperledger Fabric

In this module the block-chain concept is explain, Hyperledger Fabric is an open source framework implementation for private and permissioned business networks, designed as a foundation for developing solutions with a modular architecture. It allows components, such as ledger database, consensus mechanism and membership services, to be plug-and-play. And delivers enterprise-ready network security, scalability, confidentiality.

A. Writing Chaincode

In this module of writing chaincode, you define the architecture for your business application by defining users, entities, permissions of what they are allowed to do and the main functionality of the blockchain application which would be the logic. Combining all of it a .bna file is created which acts as a package for your blockchain application.

A. Generating Rest Server

Rest server that helps you host your business application that would display in JSON format which isn't user friendly. Yeoman generator which helps you create or build an angular application for the same application is more user friendly and has a better user interface which can be customized for making searches and filters.

IV. WORKING

The working process of the system is as explain below:

- ✓ Firstly, Using the Hyperledger fabric a network card shall be generated by executing some commands we pull up the docker image of Hyperledger fabric that create some peers and create a channel and bring up the fabric dev servers.
- ✓ And we create a peer-admincard for the network administrator to create multiple entities and create a logic or chaincode which defines the main functionality or consensus that defines the whole project.
- ✓ After defining the model file, the logic and the permission file we create a .bna archive that will be invoked and instantiated and must be updated on the ledger for all the nodes including ordering service, clients, committer and endorser nodes.
- ✓ A composer rest server shall bind this archive file and create a scaffold to generate a JSON data on the local server.
- ✓ And with help of Yeoman a scaffold shall be generated with angular frontend thus making it user friendly for an admin to create an enterprise grade business architecture in a blockchain environment.

So, after making those operations on the block-chain, we easy understand the whole mechanism of the private and permissioned block-chain application.

V. FLOW DIAGRAM

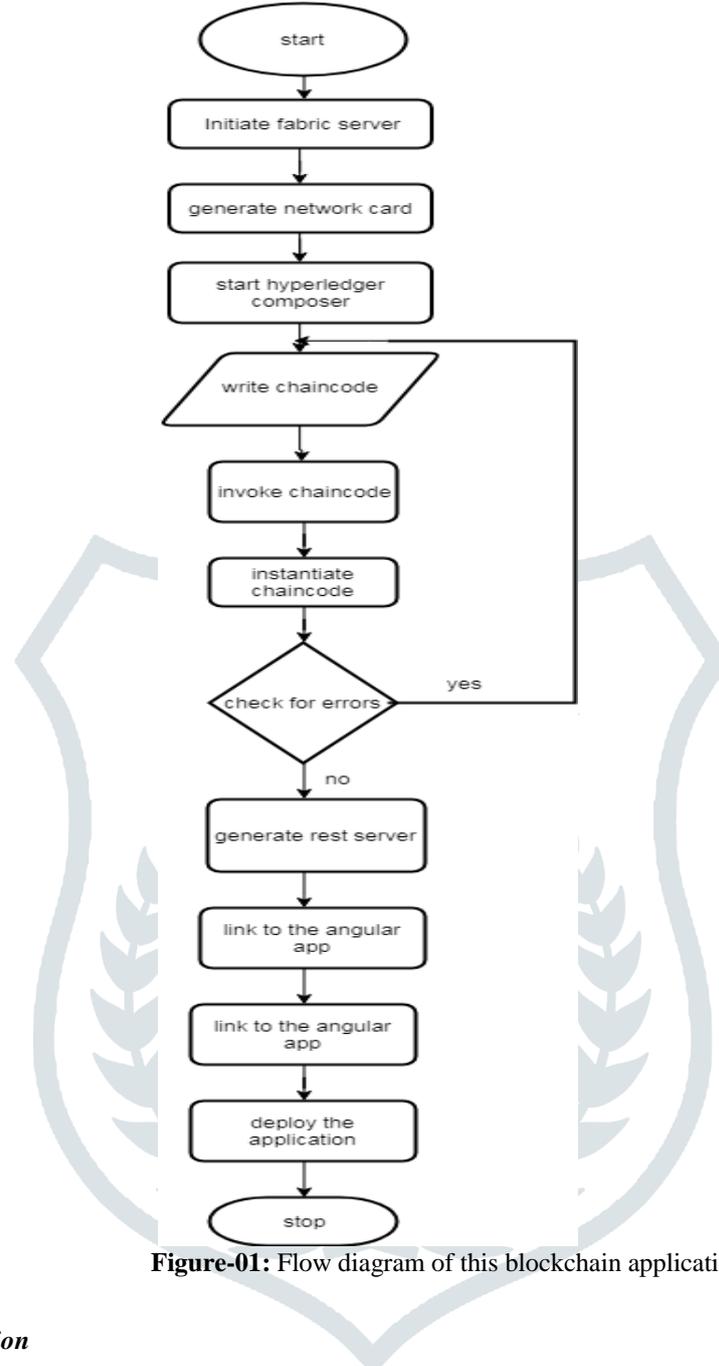


Figure-01: Flow diagram of this blockchain application

A. Flow Diagram explanation

The image in **Figure-01** is the flow diagram of how actually a private blockchain application can be built and executed.

VI. FUTURE ENHANCEMENTS

Even though the project described in this article is successful in completing its duties there are some areas or parts where this can be improve. A few points to carry on for the future have been listed below.

- 1) There is no advanced security as REST server have lot of existing security vulnerabilities which can be enhanced by a more complex server.
- 2) Can be clubbed with IoT devices to enhance the security of their operations.
- 3) Is deployed in the local server should be implemented on the internet.

VII. CONCLUSION

In conclusion even though, this paper gives a simpler explanation of private and permissioned block-chain technology, we can affirm that this is a very good point to start with one's block-chain learning journey. And in the end I can ensure that this field is too booming and it is surely the hope for many widely used real time applications ensuring confidentiality, integrity and privacy of dat.

VIII. REFERENCES**A. Research Papers**

- [1] Ittay Eyal, Adam Efe Gencer, Emin Gün Sirer, and R. Van Renesse. Bitcoin-NG: A Scalable Blockchain Protocol. Usenix Conference on Networked Systems Design and Implementation, ser. NSDI'16. Berkeley, CA, USA. USENIX Association. 2016
- [2] Linux Foundation Unites Industry Leaders to Advance Blockchain Technology - The Linux Foundation". The Linux Foundation. 2015-12-17. Retrieved 2018-04-28.
- [3] "hyperledger/fabric". GitHub. Retrieved 2016-06-23.
- [4] Keirns, Garrett. "Monax Adds Blockchain Code to Hyperledger GitHub Repository". Coindesk. Coindesk. Retrieved 12 April 2017.
- [5] "Hyperledger Composer - Hyperledger". Hyperledger. Retrieved 2018-04-28

B. Web References

- <https://hyperledger.github.io/composer/v0.19/installing/installing->
<https://hyperledger.github.io/composer/v0.19/applications/applications-index>
<https://medium.com/coinmonks>

