

Introduction to Hyperledger Fabric

 ddas.tech/introduction-to-hyperledger-fabric/

April 13, 2023

Created By: Debasis Das (Apr-2023)

Table of Contents

- [What is a Blockchain?](#)
- [What is a Blockchain Network?](#)
- [What are Smart Contracts?](#)
- [What is Hyperledger Fabric](#)
- [What are the modularity features of Hyperledger Fabric](#)
- [Permissioned vs Permissionless Blockchains](#)
- [Pluggable Consensus Protocol](#)
- [Whats new in Fabric 2.0](#)
- [Key Concepts of Hyperledger Fabric](#)
 - [Hyperledger Fabric Membership Service Provider \(MSP\)](#)
 - [Fabric Policies](#)
 - [Ordering Services](#)
- [Summary](#)
- [References](#)

What is a Blockchain?

- Blockchain is an immutable transaction ledger maintained within a distributed network of peer nodes. Each node maintains a copy of the ledger by applying transactions that have been validated by a consensus protocol.
- Bitcoin Cryptocurrency is the most widely recognized application of blockchain.

What is a Blockchain Network?

- A technical infrastructure that provides ledger and smart contract (chaincode) services to applications.
- Primarily, smart contracts are used to generate transactions which are subsequently distributed to every peer node in the network where they are immutably recorded on their copy of the ledger.

What are Smart Contracts?

- Smart contracts are self-executing contracts that are built on top of blockchain technology. They are computer programs that automatically execute the terms of a contract when certain conditions are met.
- Smart contracts are stored on the blockchain, which makes them transparent, tamper-proof, and immutable.
- They enable parties to enter into agreements without the need for intermediaries.

What is Hyperledger Fabric

- Is an open-source permissioned blockchain platform that allows developers to create and manage private, decentralized blockchain networks.
- Is a enterprise-grade permissioned distributed ledger technology (DLT) platform
- Is hosted by the Linux Foundation and includes a range of blockchain-related technologies.
- Provides a modular architecture that allows developers to customize the platform to their specific requirements. It supports a range of consensus algorithms, including **pluggable consensus protocols**, and allows for the use of smart contracts written in a variety of programming languages.
- **Supports private permissioned blockchain networks.** This means that network participants must be authenticated and authorized to access the network
- **Well-suited for enterprise** use cases where **privacy** and security are important.
- Hyperledger Fabric is scalable to large number of transactions, modular (allowing customizations), Privacy (Supports private permission blockchain networks) and allows use of Smart Contracts written in various programming languages

What are the modularity features of Hyperledger Fabric

- Pluggable ordering service (establishes a consensus on the order of transactions and broadcasts to the peers)
- Pluggable membership service provider (responsible for associating entities in the network with cryptographic identities.
- Peer to Peer gossip service
- Smart Contracts that can be written in standard programming languages.
- Pluggable endorsement and validation policy enforcement.

Permissioned vs Permissionless Blockchains

- In a **permissioned blockchain** the access to the network is restricted to a group of authorized participants. In a permissioned blockchain, the participants have control over the validation of transactions and the management of the network. Permissioned blockchains are typically used in private settings, such as within a company or between a group of organizations where the participants need to have a higher level of control and privacy.

- **Permissionless blockchain** is open to anyone who wants to participate in the network. There are no restrictions on who can join, and the participants are not required to follow any specific rules or protocols to participate. Mostly used in public setting.

Pluggable Consensus Protocol

- Consensus is the process by which a network of nodes in a blockchain system agrees on the validity of transactions and updates to the shared ledger.
- Different consensus algorithms have different trade-offs in terms of security, speed, and resource requirements.
- **Pluggable Consensus Protocol** Enables developers to choose from a range of consensus algorithms to suit their specific use cases.
- Hyperledger Fabric supports the following Pluggable Consensus protocols
 - **Kafka Ordering Service (KAFKA)**: Order Transactions before they are committed to the ledger. Is highly scalable and is fault tolerant. Suitable for large scale deployments
 - **Raft Ordering Service (RAFT)**: Uses the Raft algorithm to order transactions. Designed for use in smaller networks.
 - **Solo Ordering Service (SOLO)**: Simple consensus protocol that does not require a network of nodes to agree on transaction ordering. Often used for testing and development purposes.
 - **Practical Byzantine Fault Tolerance (PBFT)**: Highly secure and fault-tolerant, even in the presence of malicious actors. Often used in permissioned networks where the identities of network participants are known and trusted.

Whats new in Fabric 2.0

- Supports both centralized trust models and decentralized trust models requiring a sufficient number of organizations to agree on an endorsement policy.
- Multiple organizations have to agree on the chain code upgrade.
- It now has a simpler endorsement policy and private data collection updates.
- Inspectable chaincode packages.
- Allows starting multiple chain codes on a channel using one package

Key Concepts of Hyperledger Fabric

Following are few of the key concepts of the Hyperledger Fabric.

Hyperledger Fabric Membership Service Provider (MSP)

- Hyperledger Fabric Membership Service Provider (MSP) is a component of the Hyperledger Fabric blockchain framework that manages identities of network participants. MSP is responsible for ensuring that each participant in the network is authorized to participate and has the appropriate permissions.
- MSPs provide a way to authenticate the identity of each participant in the network and to ensure that only authorized participants can access sensitive information or perform certain actions on the blockchain.
- MSPs are responsible for ***Identity Management, Authentication, Authorization and Membership Revocation***

Fabric Policies

- Set of rules and procedures that govern the behavior of participants in the network.
- Policies are used to control access to resources, manage transactions, and ensure the overall security and integrity of the blockchain.
- In Hyperledger Fabric, policies are implemented using the Fabric Policy Language (FPL), which is a domain-specific language designed to express complex policies in a clear and concise manner.

Different types of policies in Hyperledger Fabric, including:

- **Endorsement policies** – Criteria that must be met before a transaction can be endorsed
- **Access control policies**- Control access to resources in the network, such as assets or smart contracts.
- **Validation policies**: Criteria that must be met before a block can be added to the blockchain.
- **Membership policies**: Used to manage the membership of participants in the network.

Ordering Services

- Responsible for ordering and validating transactions before they are committed to the blockchain. The ordering service is also known as the Consensus Service in Hyperledger Fabric.
- Ordering service ensures the consistency and validity of the blockchain by enforcing the consensus rules that are agreed upon by the network participants.
- The consensus algorithm used by the ordering service determines the order in which transactions are added to the blockchain and ensures that all participants in the network agree on the order.

- Hyperledger Fabric provides pluggable consensus mechanisms, which means that different consensus algorithms can be used based on the specific needs of the network. Some of the consensus algorithms supported by Hyperledger Fabric include:
 - **Kafka-based ordering service:** This is the default consensus mechanism used in Hyperledger Fabric, which uses the Apache Kafka messaging system for ordering transactions.
 - **Raft-based ordering service:** This is an alternative consensus mechanism that uses the Raft algorithm for ordering transactions. Raft is a widely used consensus algorithm that provides fault tolerance and strong consistency guarantees.

Summary

Hyperledger Fabric is a complex blockchain framework that is designed to support enterprise-level applications.

- **Architecture:** Hyperledger Fabric has a modular architecture that separates the roles of participants in the network. The architecture includes multiple components, such as peer nodes, ordering service, membership service provider, and chaincode, which work together to provide a scalable and secure blockchain network.
- **Permissioned blockchain:** Hyperledger Fabric is a permissioned blockchain, which means that access to the network is restricted to authorized participants. This is in contrast to permissionless blockchains, such as Bitcoin, where anyone can participate in the network.
- **Consensus mechanisms:** Hyperledger Fabric supports pluggable consensus mechanisms, which means that different consensus algorithms can be used based on the specific needs of the network. This provides flexibility in choosing the most appropriate consensus mechanism for a particular use case.
- **Chaincode:** Hyperledger Fabric uses chaincode, which is similar to smart contracts in other blockchain frameworks. Chaincode is used to define the rules and logic for interacting with assets on the blockchain.
- **Membership service provider (MSP):** Hyperledger Fabric uses MSP to manage identities of network participants. MSP is responsible for ensuring that each participant in the network is authorized to participate and has the appropriate permissions.
- **Endorsement policies:** Hyperledger Fabric uses endorsement policies to ensure that transactions meet specific requirements before they are executed on the blockchain. Endorsement policies specify the criteria that must be met before a transaction can be endorsed by a participant in the network.
- **Channel architecture:** Hyperledger Fabric supports multiple channels, which allow different subsets of participants to transact privately and securely. Channels are used to isolate sensitive information and transactions from other participants in the network.

References

<https://hyperledger-fabric.readthedocs.io/en/release-2.2/whatis.html>