Hyperledger Fabric Fundamentals

Swetha Repakula
Open Source Contributor, IBM Open Technologies
srepaku@us.ibm.com
@swayr93

Morgan Bauer
Open Source Contributor, IBM Open Technologies
mbauer@us.ibm.com
@ibmhb
Hyperledger Modular Approach

Frameworks
- **Hyperledger Burrow**: Permissionable smart contract machine (EVM)
- **Hyperledger Fabric**: Permissioned with channel support
- **Hyperledger Grid**: WebAssembly-based project for building supply chain solutions
- **Hyperledger Indy**: Decentralized Identity
- **Hyperledger Iroha**: Mobile application focus
- **Hyperledger Sawtooth**: Permissioned & permissionless support; EVM transaction family

Tools
- **Hyperledger Caliper**: Blockchain framework benchmark platform
- **Hyperledger Cello**: As-a-service deployment
- **Hyperledger Composer**: Model and build blockchain networks
- **Hyperledger Explorer**: View and explore data on the blockchain
- **Hyperledger Quilt**: Ledger interoperability
- **Hyperledger Ursa**: Shared Cryptographic Library
Introducing Blockchain for Business
Food Trust

What?
- Provide a trusted source of information and traceability to improve transparency and efficiency across the food network.

How?
- Shared ledger for storing digital compliance documentation, test results and audit certificates network.

Benefits
- Reduce impact of food recalls through instant access to end-to-end traceability data to verify history in the food network and supply chain.
- Help to address the 1 in 10 people sickened and 400,000 fatalities which occur every year from food-born illnesses.
What is Hyperledger Fabric

• An implementation of blockchain technology that is intended as a foundation for developing blockchain applications for the enterprise

• Key characteristics:
  – Permissioned
  – Highly modular
    • Pluggable consensus, ledger, membership services, endorsement and validation
  – Smart contracts in general purpose languages
  – Privacy
  – No “mining” or native crypto-currency required for consensus
  – Execute-order-validate vs order-execute
Technical Deep Dive

• [ Architectural Overview ]
• Network Consensus
• Channels and Ordering Service
• Components
• Network setup
• Endorsement Policies
• Membership Services
• Roadmap
Hyperledger Fabric V1 Architecture

Client Application

SDK (HFC)

External-CA

Fabric-CA

Membership Services

optional

Peer

Admin

Hyperledger Fabric Network

Ordering-Service

Endorser

Committer

Ledger

Chaincode

Events
How applications interact with the ledger

1. Client Application in using Hyperledger Fabric Client (HFC) SDK

2. Smart Contract implemented using chaincode – managing the World state
The Fabric ledger is maintained by each peer and includes the blockchain and worldstate.

A separate ledger is maintained for each channel the peer joins.

Transaction read/write sets are written to the blockchain.

Channel configurations are also written to the blockchain.

The worldstate can be either LevelDB (default) or CouchDB:
  - LevelDB is a simple key/value store
  - CouchDB is a document store that allows complex queries

The smart contact Contract decides what is written to the worldstate.
Technical Deep Dive

• Architectural Overview
• [ Network Consensus ]
• Channels and Ordering Service
• Components
• Network setup
• Endorsement Policies
• Membership Services
• Roadmap
## Nodes and roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Committing Peer</strong></td>
<td>Maintains ledger and state. Commits transactions. May hold smart contract (chaincode).</td>
</tr>
<tr>
<td><strong>Endorsing Peer</strong></td>
<td>Specialized peer also endorses transactions by receiving a transaction proposal and responds by granting or denying endorsement. Must hold smart contract.</td>
</tr>
<tr>
<td><strong>Ordering Node</strong></td>
<td>Approves the inclusion of transaction blocks into the ledger and communicates with committing and endorsing peer nodes. Does not hold smart contract. Does not hold ledger.</td>
</tr>
</tbody>
</table>
Consensus is achieved using the following transaction flow:
Application proposes transaction

Endorsement policy:
• “E₀, E₁ and E₂ must sign”
• (P₃, P₄ are not part of the policy)

Client application submits a transaction proposal for Smart Contract A. It must target the required peers \{E₀, E₁, E₂\}
Sample transaction: Step 2/7 – Execute proposal

E₀, E₁ & E₂ will each execute the proposed transaction. None of these executions will update the ledger.

Each execution will capture the set of Read and Written data, called RW sets, which will now flow in the fabric.

Transactions can be signed & encrypted.
Sample transaction: Step 3/7 – Proposal Response

Application receives responses

RW sets are asynchronously returned to application

The RW sets are signed by each endorser, and also includes each record version number

(This information will be checked much later in the consensus process)

Key:
- **Endorser**
- **Ledger**
- **Application**
- **Ordering Node**
- **Endorsement Policy**

Hyperledger Fabric Network
Sample transaction: Step 4/7 – Order Transaction

Responses submitted for ordering

Application submits responses as a transaction to be ordered.

Ordering happens across the fabric in parallel with transactions submitted by other applications.

Key:
- Endorser
- Ledger
- Committing Peer
- Application
- Ordering Node
- Application
- Endorsement Policy
- Smart Contract (Chaincode)

Hyperledger Fabric Network

(Other applications)
Sample transaction: Step 5/7 – Deliver Transaction

Orderer delivers to committing peers

Ordering service collects transactions into proposed blocks for distribution to committing peers. Peers can deliver to other peers in a hierarchy (not shown)

Different ordering algorithms available:
- SOLO (Single node, development)
- Kafka (Crash fault tolerant)
- Raft (Crash fault tolerant)
Sample transaction: Step 6/7 – Validate Transaction

Committing peers validate transactions

Every committing peer validates against the endorsement policy. Also check RW sets are still valid for current world state

Validated transactions are applied to the world state and retained on the ledger

Invalid transactions are also retained on the ledger but do not update world state
Sample transaction: Step 7/7 – Notify Transaction

Applications can register to be notified when transactions succeed or fail, and when blocks are added to the ledger.

Applications will be notified by each peer to which they are connected.

Key:
- Endorser
- Ledger
- Committing Peer
- Application
- Ordering Node
- Ordering-Service
- Smart Contract (Chaincode)
- Endorsement Policy
Technical Deep Dive

- Architectural Overview
- Network Consensus
- [Channels and Ordering Service]
- Components
- Network setup
- Endorsement Policies
- Membership Services
- Roadmap
Ordering Service

The ordering service packages transactions into blocks to be delivered to peers. Communication with the service is via channels.

Different configuration options for the ordering service include:

– **Solo**
  - Single node for development

– **Kafka** : Crash fault tolerant consensus
  - 3 nodes minimum
  - Odd number of nodes recommended

– **Raft** : Crash fault tolerant
  - In-process consensus, no extra dependency
  - More decentralized, orderer nodes can be spread
Channels provide privacy between different ledgers

- Ledgers exist in the scope of a channel
  - Channels can be shared across an entire network of peers
  - Channels can be permissioned for a specific set of participants
- Chaincode is **installed** on peers to access the worldstate
- Chaincode is **instantiated** on specific channels
- Peers can participate in multiple channels
- Concurrent execution for performance and scalability
Single Channel Network

- All peers connect to the same system channel (blue).
- All peers have the same chaincode and maintain the same ledger.
- Endorsement by peers $E_0, E_1, E_2$ and $E_3$

Key:

- Endorser
- Ledger
- Committing Peer
- Application
- Ordering Node
- Smart Contract (Chaincode)
- Endorsement Policy

Hyperledger Fabric Network
Multi Channel Network

- Peers $E_0$ and $E_3$ connect to the **red** channel for chaincodes $Y$ and $Z$
- $E_1$, $E_2$ and $E_3$ connect to the **blue** channel for chaincodes $A$ and $B$

Key:
- **Endorser**
- **Ledger**
- **Committing Peer**
- **Application**
- **Ordering Node**
- **Smart Contract (Chaincode)**
- **Endorsement Policy**
Technical Deep Dive

• Architectural Overview
• Network Consensus
• Channels and Ordering Service
• Components
• Network setup
• [ Endorsement Policies ]
• Membership Services
• Roadmap
Endorsement Policies

An endorsement policy describes the conditions by which a transaction can be endorsed. A transaction can only be considered valid if it has been endorsed according to its policy.

- Each chaincode is deployed with an Endorsement Policy
- **ESCC** (Endorsement System Chaincode) signs the proposal response on the endorsing peer
- **VSCC** (Validation System Chaincode) validates the endorsements
**Endorsement Policy Syntax**

Policy Syntax: `EXPR(E, E...)`

Where `EXPR` is either AND or OR and `E` is either a principal or nested `EXPR`.

Principal Syntax: `MSP.ROLE`

Supported roles are: member and admin

Where `MSP` is the MSP ID, and `ROLE` is either “member” or “admin”.

### Example

$ peer chaincode instantiate
  -C mychannel
  -n mycc
  -v 1.0
  -p chaincode_example02
  -c '{"Args": ["init", "a", "100", "b", "200"]}'
  -P "AND('Org1MSP.member')"

Instantiate the chaincode `mycc` on channel `mychannel` with the policy `AND('Org1MSP.member')`
Endorsement Policy Examples

Examples of policies:

• Request 1 signature from all three principals
  – AND('Org1.member', 'Org2.member', 'Org3.member')

• Request 1 signature from either one of the two principals
  – OR('Org1.member', 'Org2.member')

• Request either one signature from a member of the Org1 MSP or (1 signature from a member of the Org2 MSP and 1 signature from a member of the Org3 MSP)
  – OR('Org1.member', AND('Org2.member', 'Org3.member'))
Technical Deep Dive

- Architectural Overview
- Network Consensus
- Channels and Ordering Service
- Components
- Network setup
- Endorsement Policies
- Membership Services
- [ Roadmap ]
Roadmap

Based on https://wiki.hyperledger.org/display/fabric/Hyperledger+Fabric+Roadmap - Dates determined by the Hyperledger community - (*) Subject to change

v1.0
- 07/17
- Channels
- Selective endorsement
- SOLO/Kafka orderers
- LevelDB or CouchDB

v1.1
- 03/18
- Javascript chaincode
- Connection profile
- Encryption library
- Attribute access control
- CouchDB indexes
- Channel based events

v1.2
- 07/18
- ACLs
- Service discovery
- Pluggable endorsement / validation
- Private Data Collections

v1.3
- 10/18
- State based endorsement
- Java chaincode
- CouchDB pagination
- Identity Mixer

v1.4
- 1/19
- Operational metrics and logging
- SDK and SHIM improvements
- Burrow EVM
- Long Term Service (LTS) support

v1.4.1
- 4/19
- Raft ordering
- Additional metrics

v1.4.2
- 7/19?
- Kafka to Raft migration

v2.0
- Chaincode lifecycle with decentralized management
- SDK improvements
- RAFT ordering including migration from Kafka
- Alpine based images
- Fabric
Getting started with Hyperledger Fabric

- Build Your First Network (BYFN) – Network administrator
  - A simple network with 2 organizations running 2 peers, with one channel, a simple chaincode
  - Dockerhub images
  - Uses predefined enrollment certificates and «Solo» Ordering Service

- Extend Your First Network – Network administrator
  - Adds a 3rd organization to BYFN

- Develop Your First Application – Application developer
  - A simple Node.js application

- Start in devmode (minimal set up), then move to network (several peers), and security (membersrvc)

- Several examples to start from (fabcar)
IBM Blockchain Platform

IBM Blockchain Platform is a fully integrated enterprise-ready blockchain platform designed to accelerate the development, governance, and operation of a multi-institution business network

- **Developer tools** to quickly build your blockchain application
- Hyperledger Fabric provides the ledger, which is managed through a set of intuitive operational tools
- **Governance tools** for democratic management of the business network
- Flexible deployment options, including a highly secure and performant IBM Cloud environment

![Diagram of IBM Blockchain Platform components](image-url)
Resources

  - Docs + tutorials

  - Code patterns, lectures, howtos, lab, etc

  - Blockchain 101

- IBM Blockchain Platform:
Get Involved!

Ensure the strength and longevity of a core technology to your business.

Publicly proclaim your leadership in the blockchain space.

Work with other blockchain leaders to develop and promote Hyperledger blockchain for business technologies.

Visit hyperledger.org/about/join or email info@hyperledger.org.
Thank you

Swetha Repakula
srepaku@us.ibm.com
@swayr93

Morgan Bauer
mbauer@us.ibm.com
@ibmhbb

IBM Blockchain

www.ibm.com/blockchain
developer.ibm.com/blockchain
www.hyperledger.org

© Copyright IBM Corporation 2018.