

Hyperledger Fabric

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay

November 2, 2018

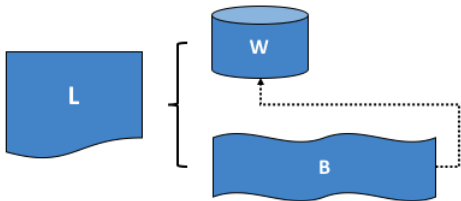
Hyperledger

- Collaborative blockchain effort hosted by Linux Foundation
- Mission
 - Create enterprise grade, open source distributed ledger frameworks
- Launched in 2016 with Fabric and Sawtooth
 - Currently 5 frameworks and 5 tools
- Companies contribute code under Apache License
 - Does not require modifications to be distributed under the same license

Hyperledger Fabric

- Permissioned distributed ledger framework with smart contracts
- Originated in IBM in mid-2015 as Open Blockchain (OBC) project
- Initial implementation completed in Dec 2015
 - 40K lines of Go code, smart contracts, PBFT consensus
- IBM joined Hyperledger in Feb 2016 and donated OBC code
- Main features
 - Members of a Fabric network enroll through a Membership Service Provider
 - A group of participants can create a channel (shared ledger)
 - Copies of the channel ledger present only with channel participants
 - Each ledger contains world state and transaction log
 - Transactions are used to update state
 - Smart contracts (called chaincode) are written in Go
 - Client SDKs available in Node.js and Java
 - Querying ledger for transactions or blocks
 - Installing chaincode in peer nodes
 - Creating transactions calling chaincode functions
 - Pluggable consensus mechanism

Ledger



	Ledger
	World State
	Blockchain
	L comprises B and W
	B determines W

Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html>

World State





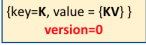
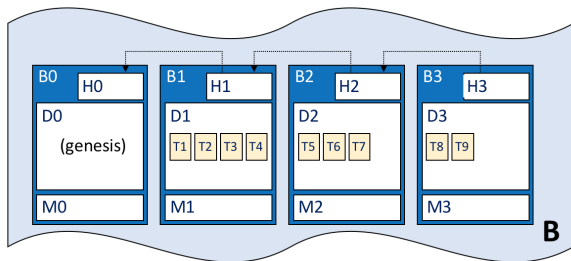
	Ledger world state
	A ledger state with key=K . It contains a set of facts expressed as a simple value, V . The state is at version 0.
	A ledger state with key=K . It contains a set of facts expressed as a set of key-value pairs {KV} . The state is at version 0.

Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html>

Blockchain



	Blockchain
	Block
	Block header
	Block data
	Transaction
	Block metadata
	H2 is chained to H1

Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html>

Blocks

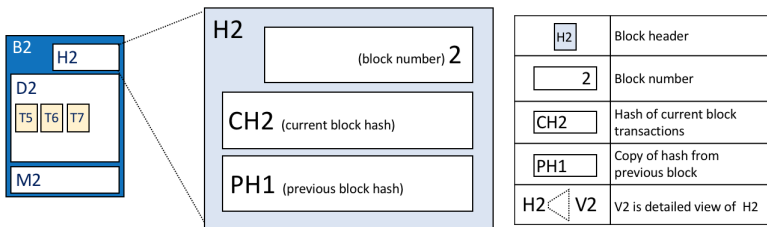
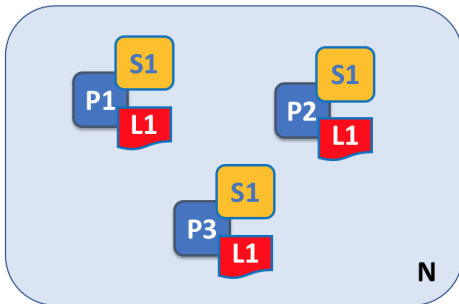


Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/ledger/ledger.html>

Peers







	Blockchain network
	Peer node
	Smart contract (aka chaincode)
	Ledger

Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html>

Multiple Ledgers and Chaincodes

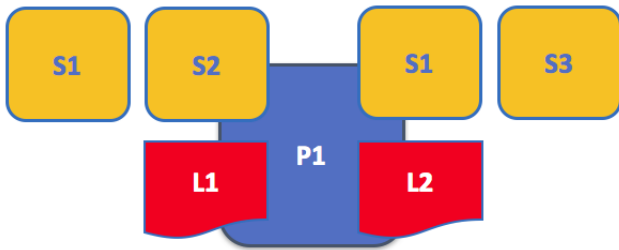


Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html>

Application-Peer Interaction

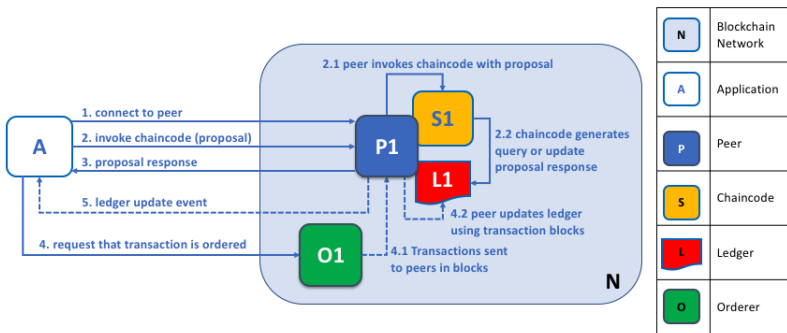
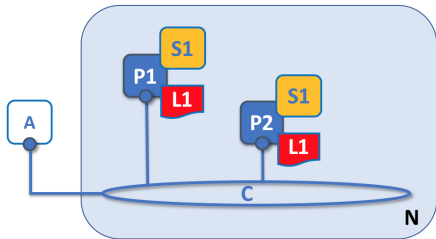


Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html>

- Ledger queries involve only first three steps
- Ledger updates involve all five steps
- Application needs to send proposed updates to several peers

Channels



	Blockchain Network		Ledger
	Channel		Application
	Peer		Principal PA (e.g. A, P1) communicates via channel C.
	Chaincode		

Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html>

Ledger Updates

Phase 1: Proposal

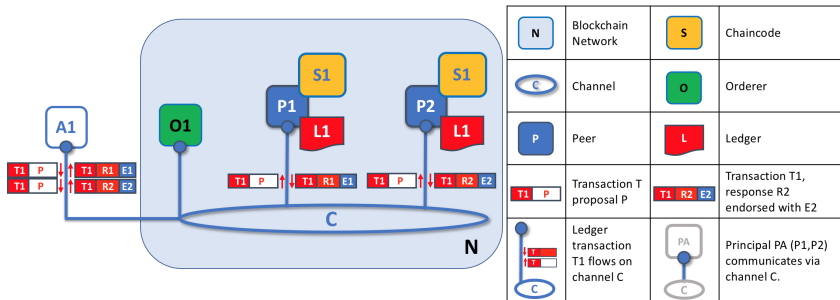


Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html>

- Application sends transaction proposal to some peers for endorsement
- Peers execute the transaction and append signatures endorsing the proposal
- Phase 1 ends when application receives sufficient responses

Ledger Updates

Phase 2: Packaging

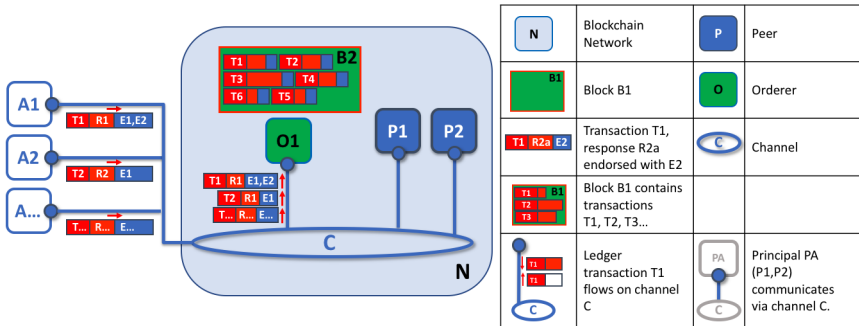
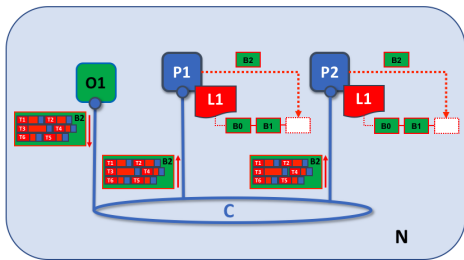


Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html>

- Endorsed transaction proposals are packaged into a block by the orderer

Ledger Updates

Phase 3: Validation













	Blockchain Network		Peer
	Channel		Orderer
	Ledger		Block B
	Ledger L1 has blockchain with blocks B0, B1		Block B1 contains transactions T1, T2, T3...
	Block B1 flows on channel C		Principal PA (P1, P2) communicates via channel C.

Image credit: <https://hyperledger-fabric.readthedocs.io/en/release-1.3/peers/peers.html>

- Orderer distributes blocks to all peers
- Each peer checks that a block satisfies the organizational endorsement policy and applies to ledger

References

- **Hyperledger** <https://eprint.iacr.org/2014/349.pdf>
- **Apache License** https://en.wikipedia.org/wiki/Apache_License
- **Fabric History** <https://www.linkedin.com/pulse/hyperledger-fabric-brief-history-binh-nguyen/>
- **Fabric Architecture** <https://arxiv.org/abs/1801.10228v1>
- **Documentation** <https://hyperledger-fabric.readthedocs.io/>