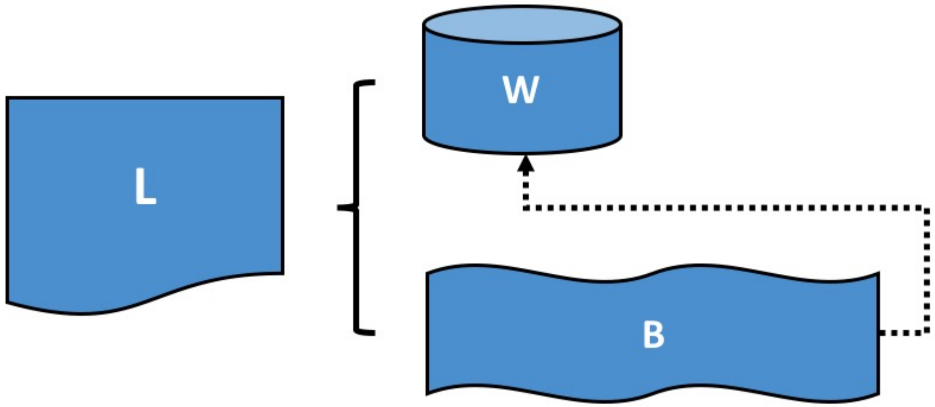
EIA Blockchain Services

Data persistence in Hyperledger Fabric

Blockchain Services

Ledger definition in HFC

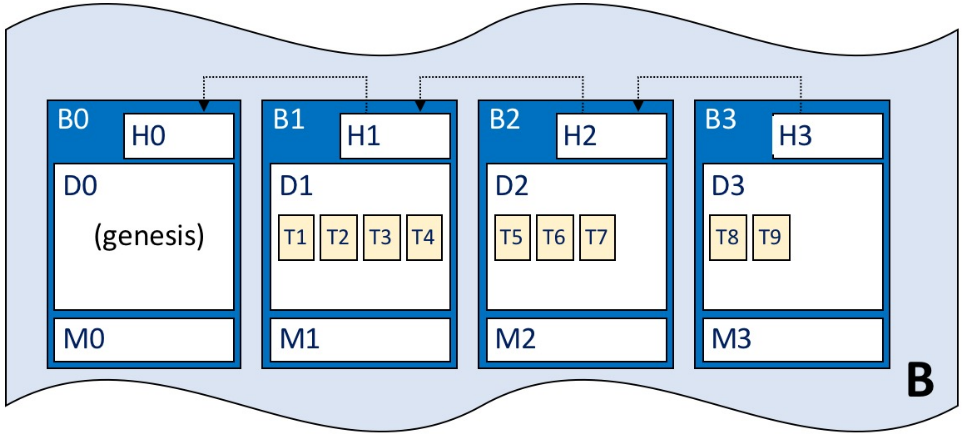
- Ledger = Blockchain + World State
- Blockchain – append only file - **immutable**
- World State – database representing current world state
- World State can be at any time reconstructed from Blockchain



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

Blockchain

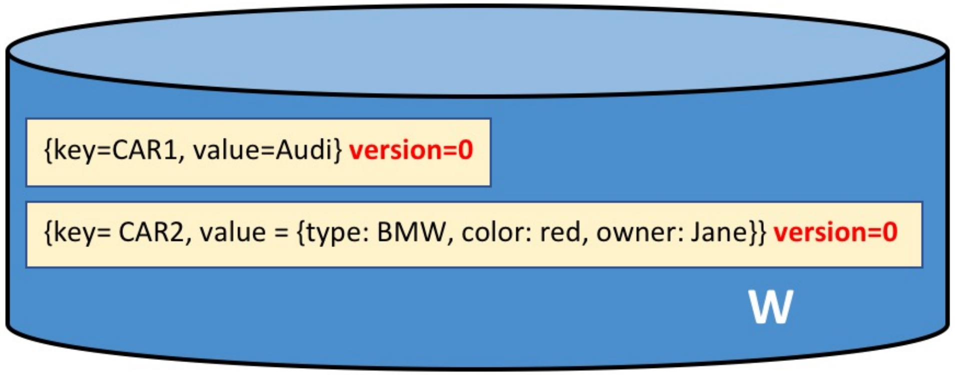
- Append only transaction log
- **Immutable**
- Consists of interlinked blocks
- Block consists of:
  - Header = block number + current block hash + previous block header hash
  - Data = list of transaction in order arranged by ordering service
  - Metadata = certificates + signature



B	Blockchain
B1	Block
H3	Block header
D1	Block data
T5	Transaction
M3	Block metadata
H1 H2	H2 is chained to H1

World state

- Database representing current world state
- Updated only on successful transactions
- Includes Key-Value pairs
- Easier search then traversing append only file
- Chaincodes works againts World State
- States can be created, updated or even **deleted**
- Can be CouchDB or LevelDB
- Can but does not have to store keys history



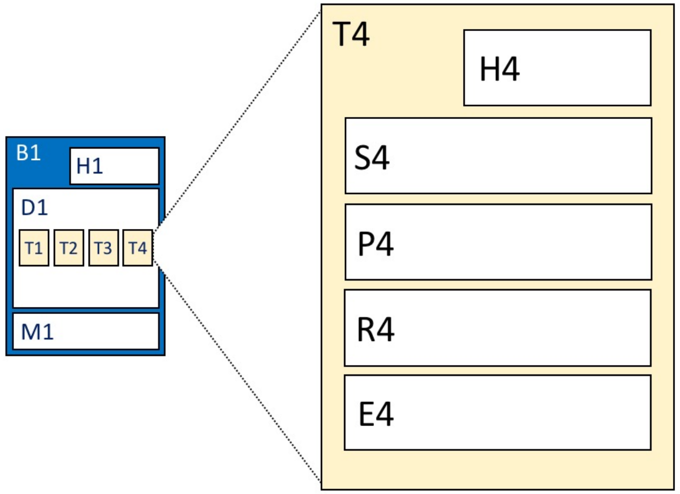
{key=CAR1, value=Audi} **version=0**

{key= CAR2, value = {type: BMW, color: red, owner: Jane}} **version=0**

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

Transaction

- Transaction captures changes to the world state
- Single block can contain multiple transactions
- Transaction consists of:
  - Header – name of chaincode, version, etc.
  - Signature – cryptographic signature created by client application
  - Proposal – Input parameters given to chaincode
  - Response – Output of chaincode invoke (also Read-Write set capturing state change)
  - Endorsement – List of signed transaction responses from organizations to statify endorsement policy
- Submit tx – append to blockfile
- Evaluate tx – only read world state



T4	Transaction
H4	Header
S4	Signature
P4	Proposal
R4	Response
E4	Endorsements
T4 ◁ V4	V4 is detailed view of T4

Chaincode namespaces

- In reality each chaincode has its own world state
- Blockchain is not namespaced
- Multiple world states representing different chaincodes can exist on single blockchain
- Chaincode can access different world state only by invoking other chaincode
- Provides data isolation between chaincodes

Channel

- Takes data isolation even further
- Each channel has completly separate Ledger (both blockchain and world state)
- Each channel has its own configuration
- Each channel consists of its own organizations consortium
- Peers needs to be eligible to join channel
- Single peer can join multiple channels
- Works almost like independent blockchain network
- Can share whole or part of ordering service with other channels

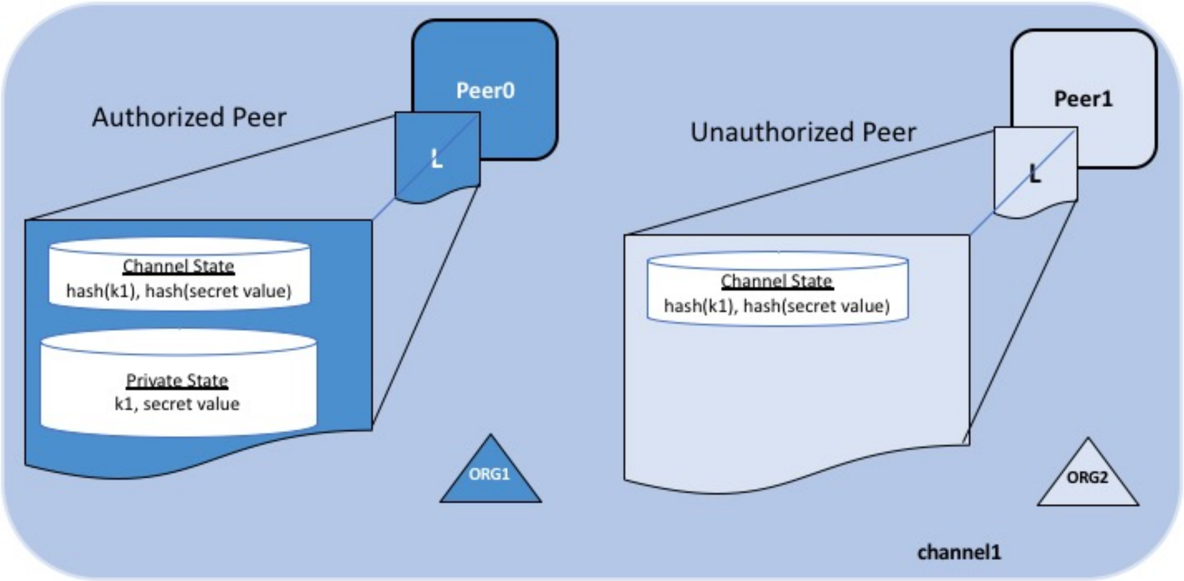
EIA Blockchain Services

Transient data

- Data passed to chaincode are stored in blockfile in transaction proposal
- Data stored in blockfile can NOT be deleted
- What if we need to pass some secret data to chaincode to execute transaction?
  - HFC allows to pass part of data as so called **Transient data**
  - Data passed to chaincode as transient are NOT stored in transcation proposal
  - Chaincode can work with transient data the same way as with standard parameters
  - Transient data can be passed alongside normal parameters.
- Used usually alongside Private data collections

Private data collection

- Additional tool for data isolation in channel
- Private data collection is seen and owned only by selected subset of organizations
- Private data are sent p2p between authorized organizations
- Ordering nodes only sees private data hashes
- Private data is stored ONLY in private state database on peers
- Private data hash is stored in channel ledger (blockchain + world state)
- Organizations with no access to private data can still validate its content againts blockchain if given private data by different means
- Private data can truly be deleted (only hash remains in ledger)



- Used images were taken from: https://hyperledger-fabric.readthedocs.io

- Thanks for all the awesome work HFC team!