# Hyperledger Fabric

21CSPH0 Blockchain Technology and Applications

# Hyperledger Fabric Model

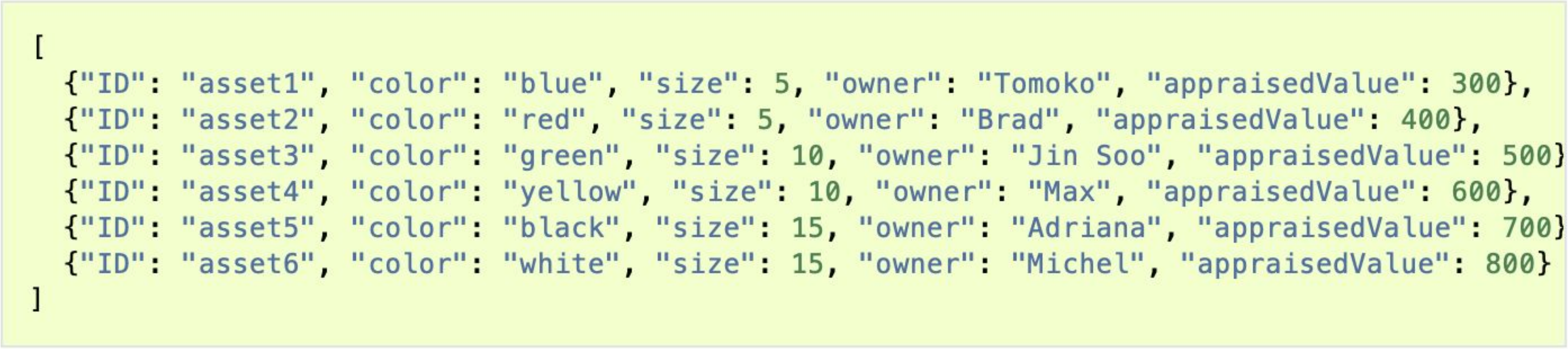
- Key design features woven into Hyperledger Fabric that fulfill its promise of a enterprise blockchain solution:
  - Assets
  - Chaincode
  - Ledger Features
  - Privacy
  - Security and Membership Services
  - Consensus

# Assets

- Tangible (real estate and hardware) or intangible (contracts and intellectual property).
- Assets are represented in Hyperledger Fabric as a collection of key-value pairs.
- Hyperledger Fabric provides the ability to modify assets using chaincode transactions.
- With state changes recorded as transactions on a channel ledger.
- Assets can be represented in binary and/or JSON form.

# Chaincode – assetTransfer

- Functionalities supported by the chaincode
  - Create, Query, Update



```
[
  {"ID": "asset1", "color": "blue", "size": 5, "owner": "Tomoko", "appraisedValue": 300},
  {"ID": "asset2", "color": "red", "size": 5, "owner": "Brad", "appraisedValue": 400},
  {"ID": "asset3", "color": "green", "size": 10, "owner": "Jin Soo", "appraisedValue": 500}
  {"ID": "asset4", "color": "yellow", "size": 10, "owner": "Max", "appraisedValue": 600},
  {"ID": "asset5", "color": "black", "size": 15, "owner": "Adriana", "appraisedValue": 700}
  {"ID": "asset6", "color": "white", "size": 15, "owner": "Michel", "appraisedValue": 800}
]
```

# Chaincode

- Chaincode is software defining an asset or assets, and the transaction instructions for modifying the asset(s) - it’s the business logic.
- Chaincode enforces the rules for reading or altering key-value pairs or other state database information.
- Chaincode functions are initiated through a transaction proposal.
- Chaincode execution results in a set of key-value writes (write set) that can be submitted to the network and applied to the ledger on all peers.

# Privacy

- *Channels* allow a subset of parties to communicate without the other members even knowing the existence of such a channel
- *SideDB* for the participants to store sensitive information locally, with only the hashes of private information stored on-chain
- *Identity Mixer* / *Idemix* to anonymize the clients with a zero-knowledge proof based signature scheme

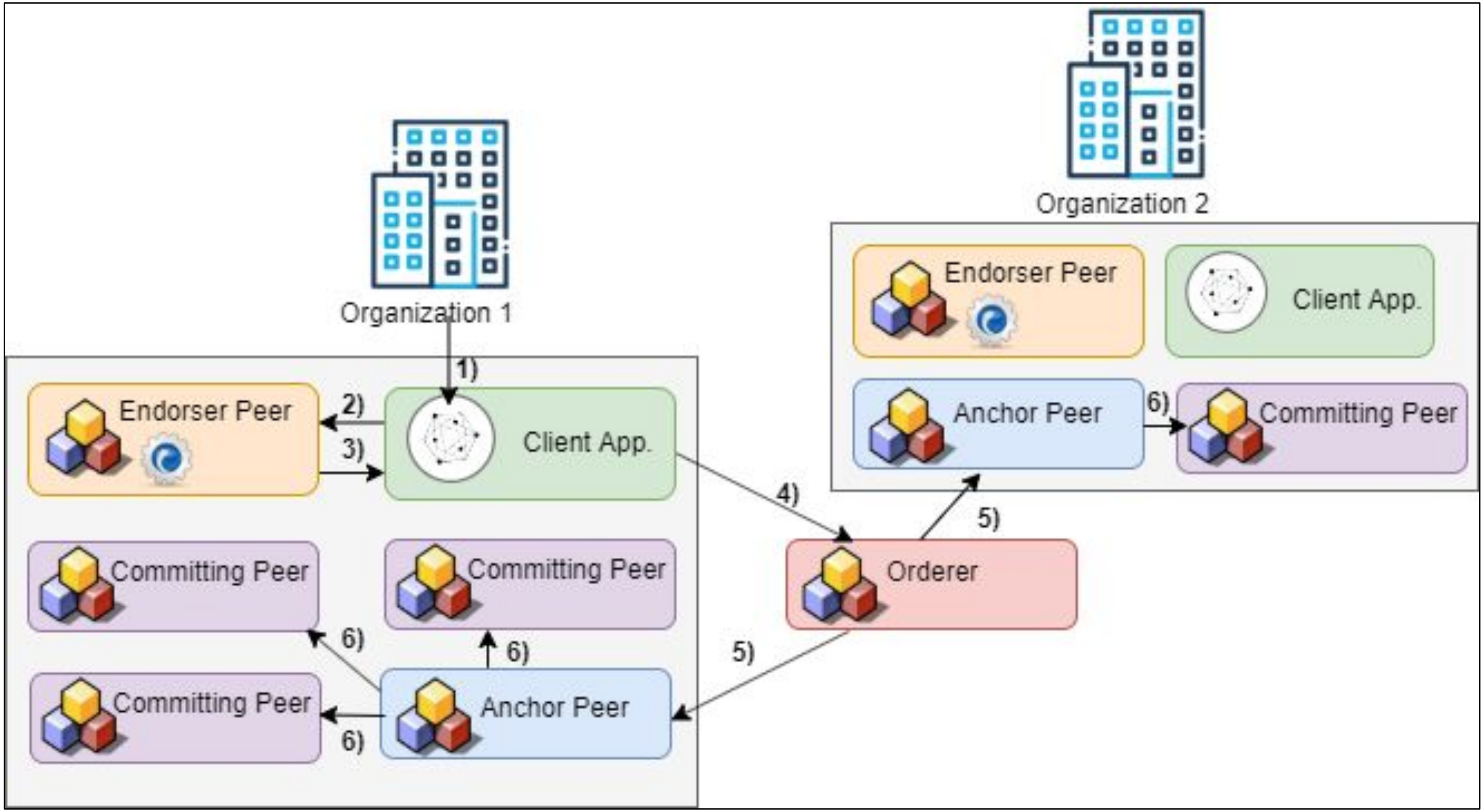
# Security and Membership Services

- Hyperledger Fabric underpins a transactional network where all participants have known identities.
- Public Key Infrastructure (PKI) is used to generate cryptographic certificates which are tied to organizations, network components, and end users or client applications.

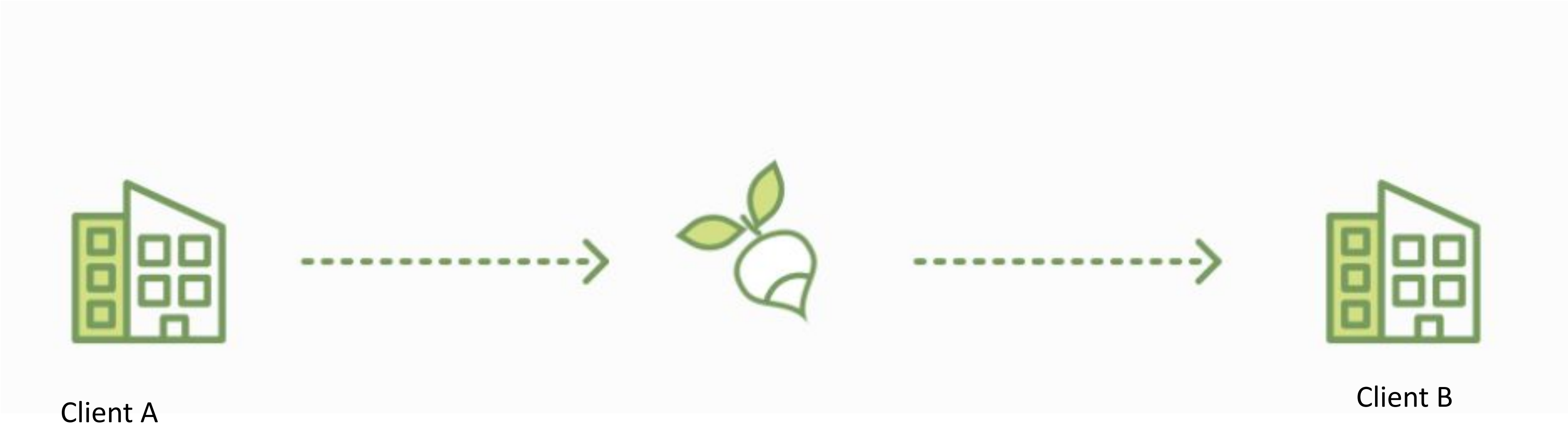
# Nodes in Hyperledger Fabric

- Client
  - Initiates the transaction request
  - Forwards it to the designated peers
- Peers
  - Endorser Peers
    - Executes the chaincode in regard to the transaction request
  - Committing Peer
- Orderer

# Hyperledger Fabric Workflow



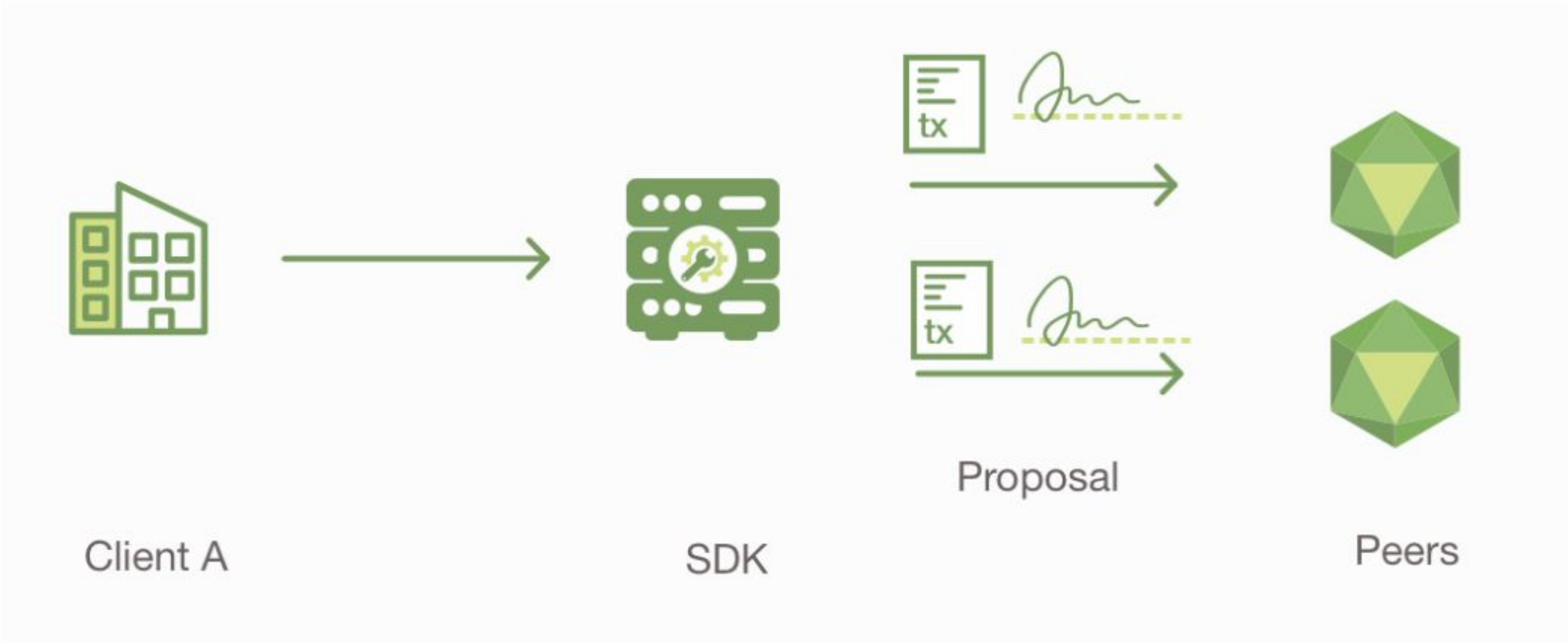
# Workflow - An Illustration



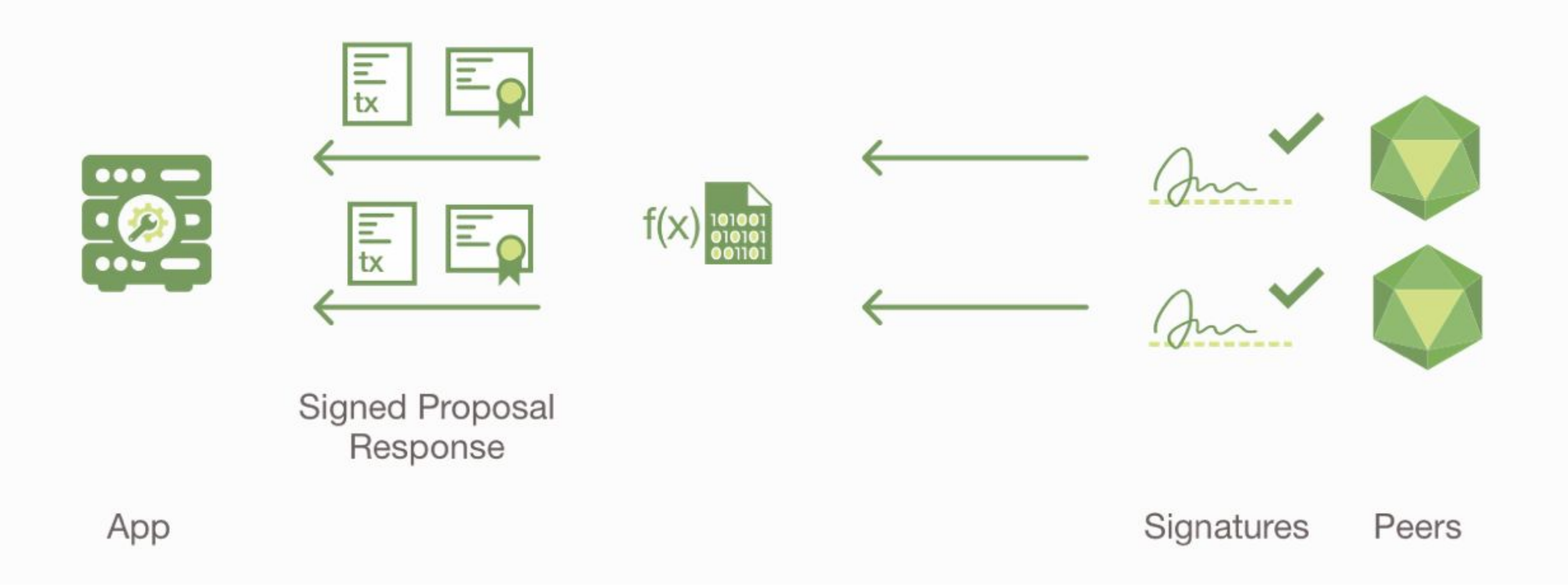
Client A

Client B

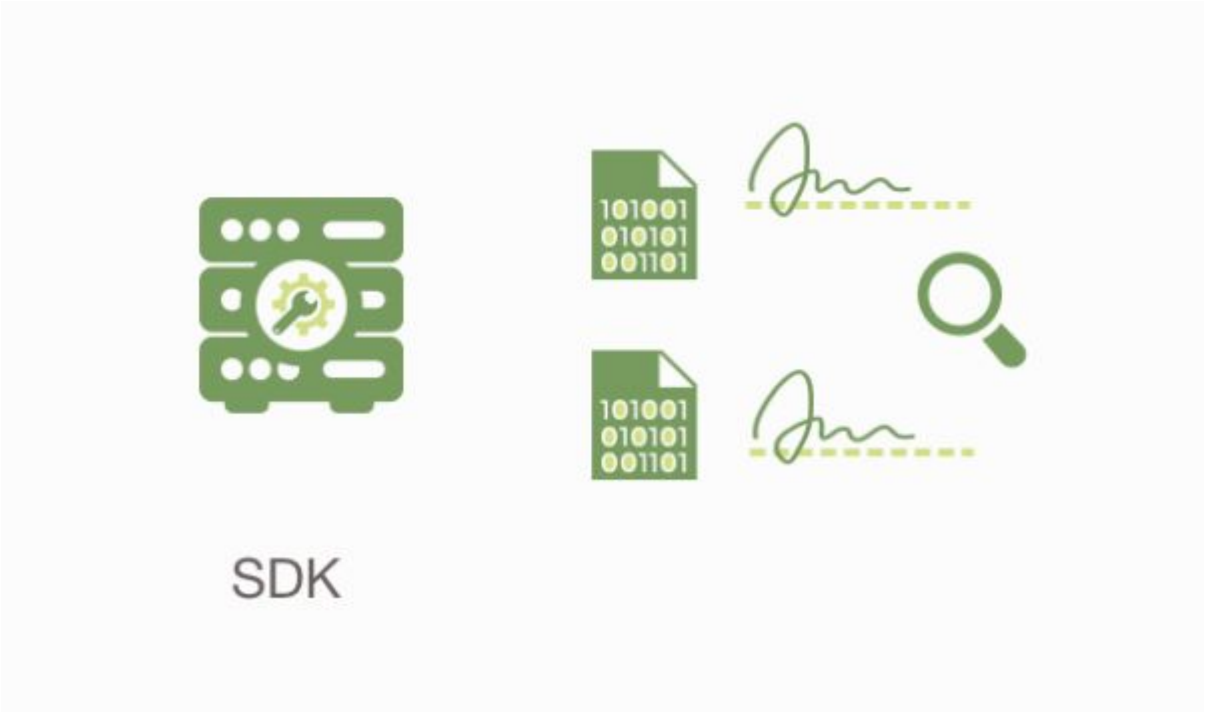
# Client A initiates a transaction



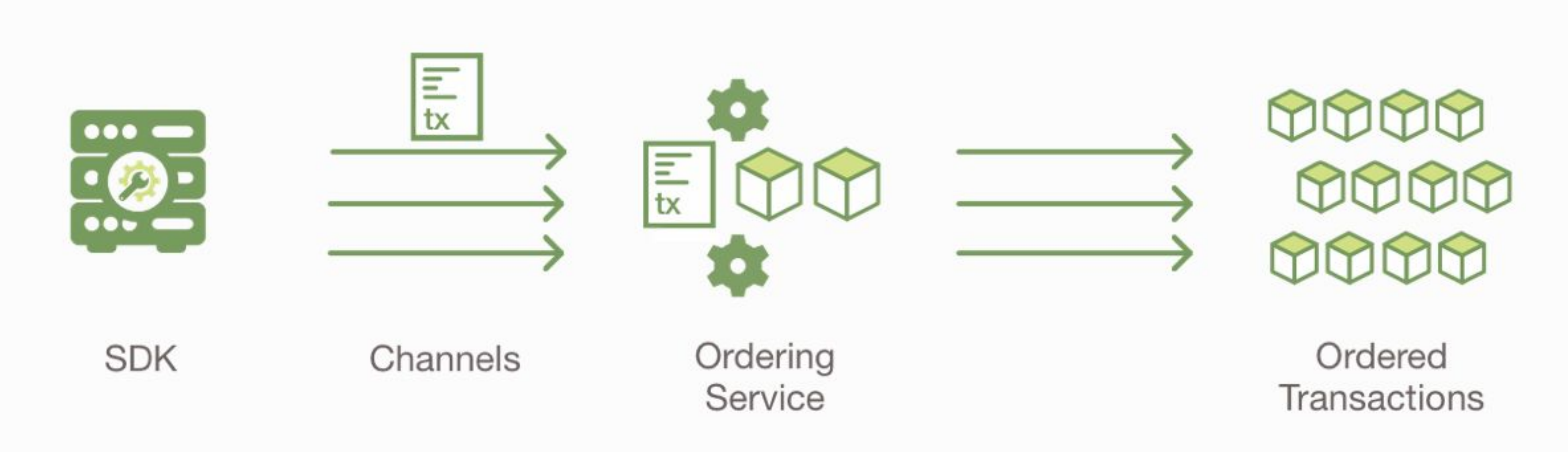
# Endorsing peers verify the signature and execute the transaction



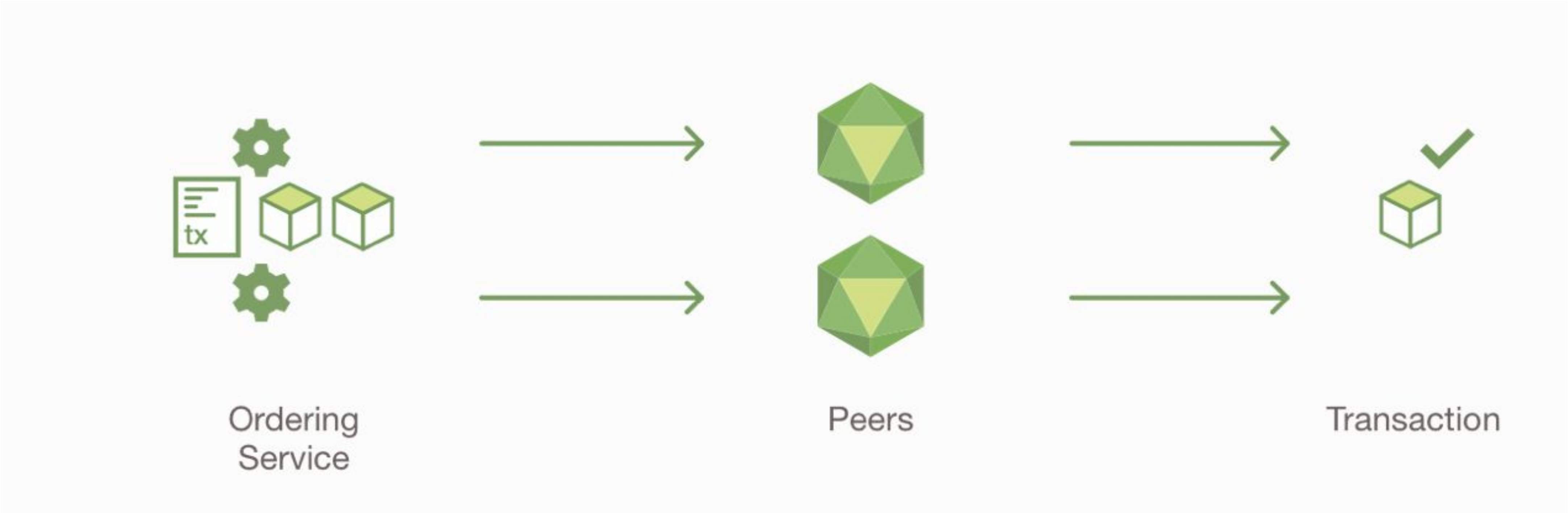
# Proposal responses are inspected



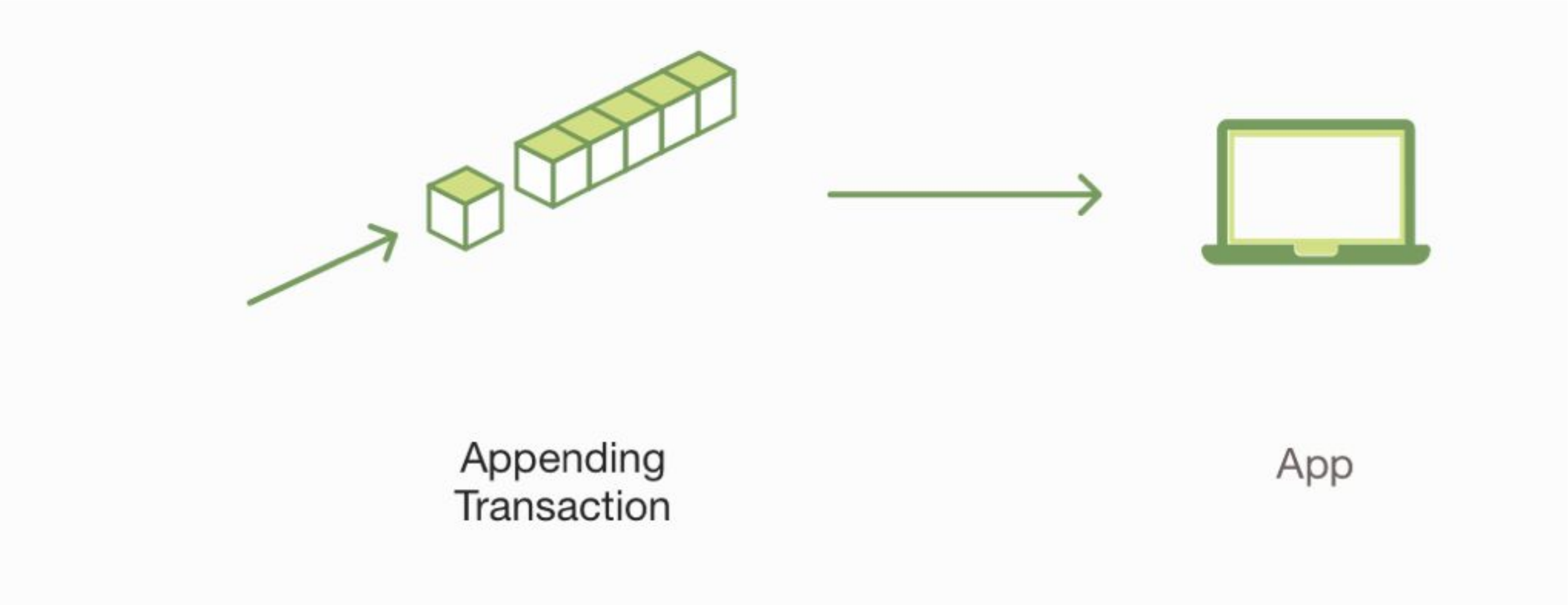
# Transaction response forwarded to the ordering service



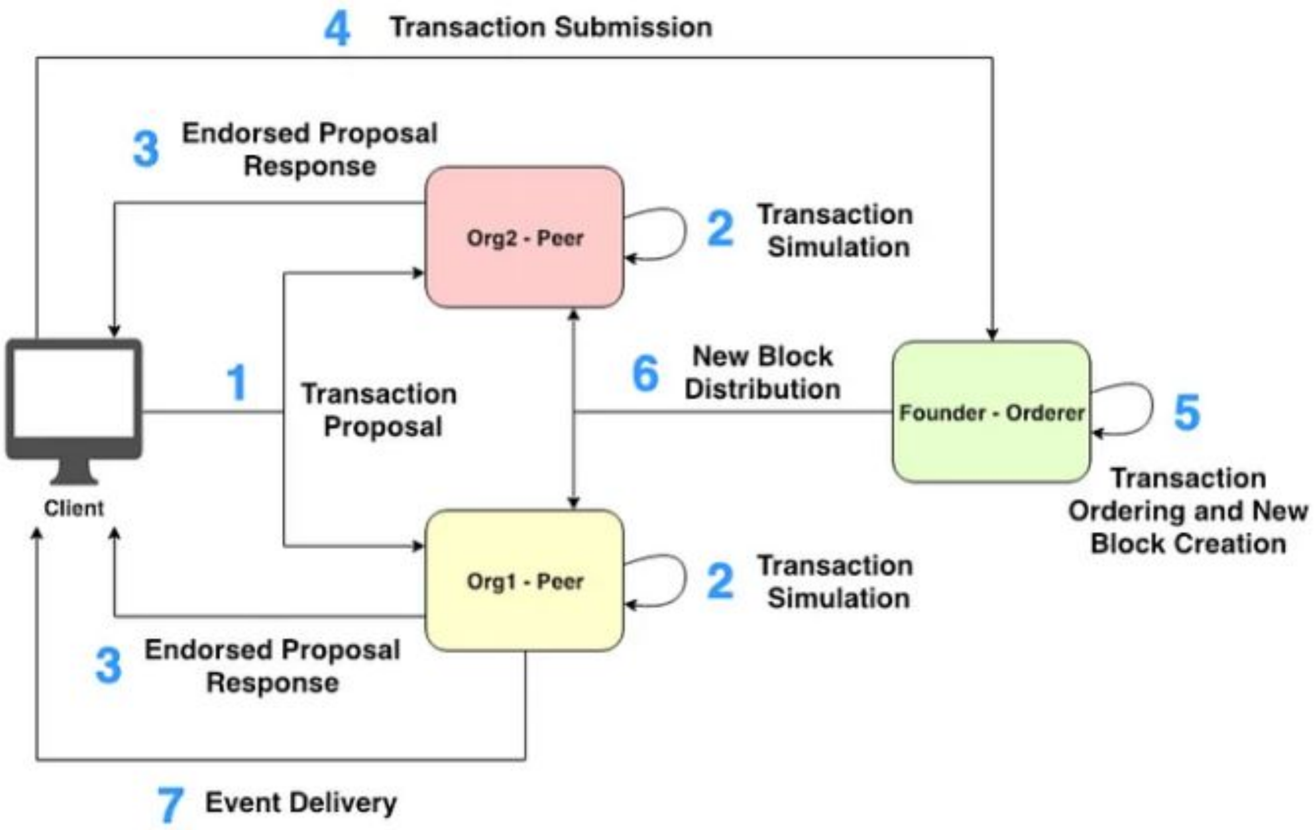
# Transaction is validated and committed



# Ledger Updated



# Hyperledger Fabric Workflow



# Endorsement Policy

- *Not all peers* execute the chaincode but only a subset based on the endorsement policy performs execution.
- Endorsement policy is a monotone logical expression of policy principals such as ”two out of three” or ”$(Org1.peer \vee Org2.peer) or (Org1.member \wedge Org3.member)$”.
- By allowing only a subset of the endorsers to execute a transaction fine grained privacy is guaranteed as other permissioned blockchain frameworks require all the nodes in the network to execute the transaction.

# References

- https://hyperledger-fabric.readthedocs.io/en/release-2.5/