QCon 全球软件开发大会
INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

BEIJING 2018

用Ethereum设计联盟链系统

ThoughtWorks中国区块链实践负责人 刘尚奇

主办方 Geekbang. 极客邦科技 InfoQ

GTLC
GLOBAL
TECH LEADERSHIP
CONFERENCE

全球技术领导力峰会

通往**年薪百万**的CTO的路上，
如何打造自己的技术**领导**力？

扫描二维码了解详情

刘尚奇

刘尚奇是ThoughtWorks全球技术战略委员会成员，中国区区块链实践负责人。致力于将区块链技术引入企业上下文，激发技术驱动的业务创新。
redecentralization运动的拥护者。

Agenda

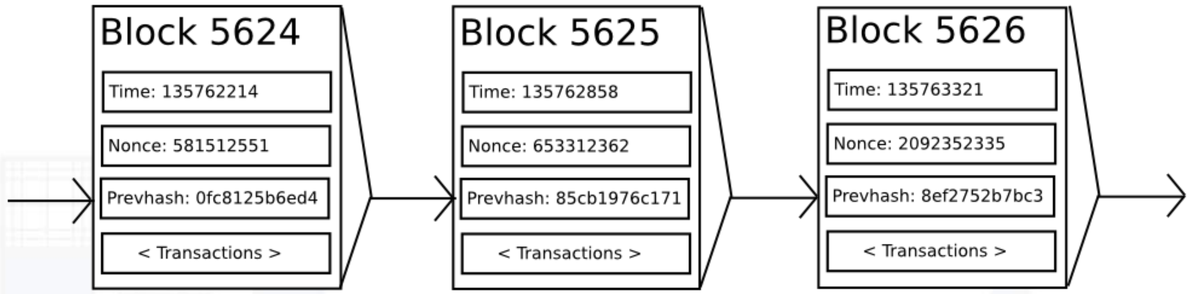
- Why start from Ethereum
- Challenage to achieve consortium blockchain
- Real world consortium blockchain

Why

ethereum

Ethereum技术特点

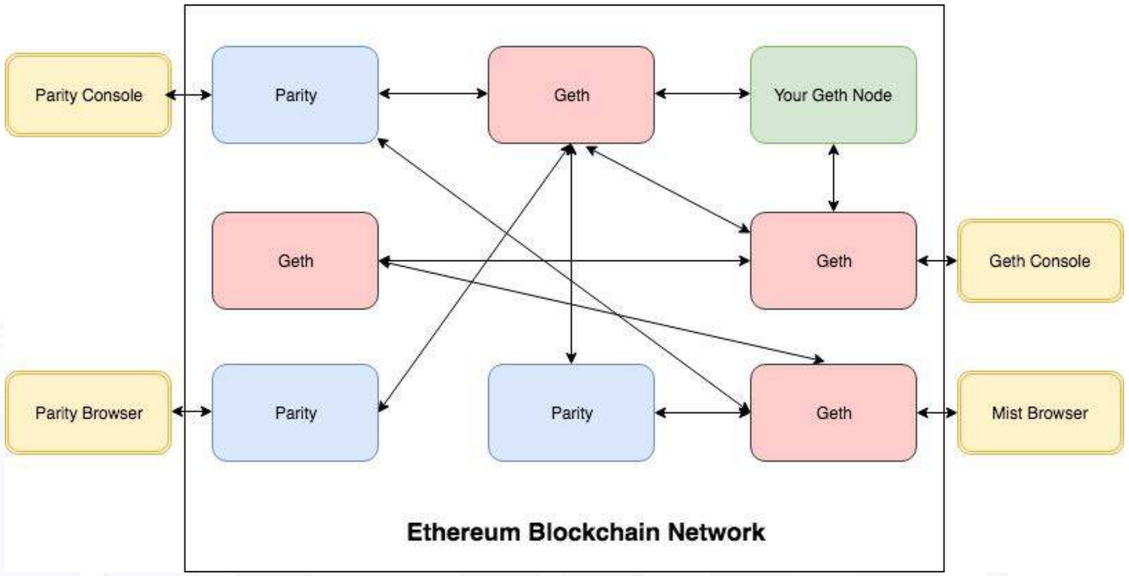
- It is (a) blockchain!
- Permissionless P2P Networking
- PoW based consensus
- All-in-one implementation



https://github.com/ethereum/wiki/wiki/White-Paper#mining

Ethereum技术特点

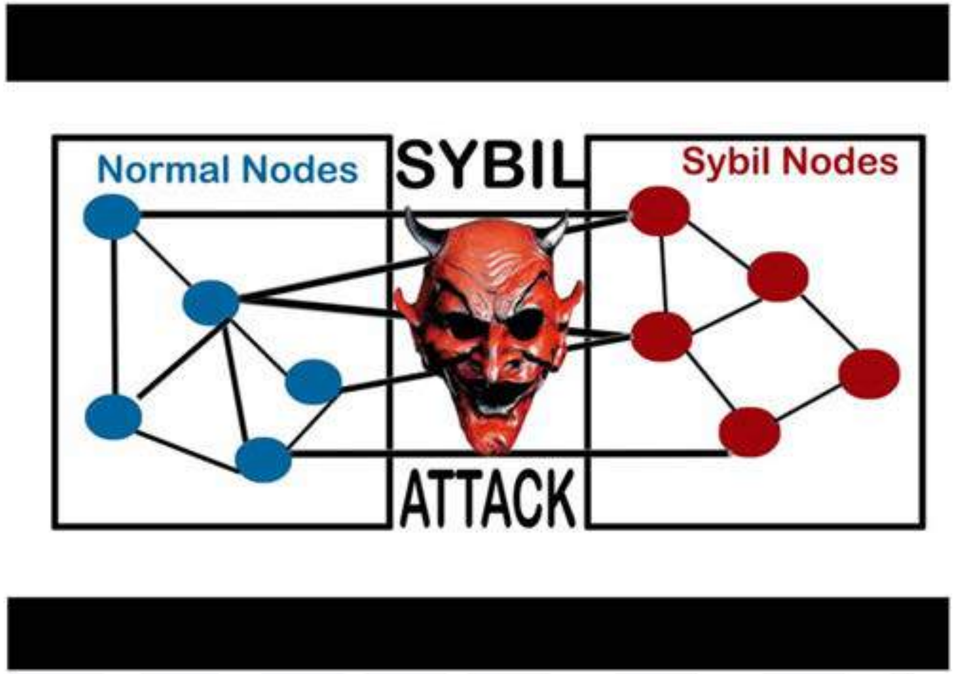
- It is (a) blockchain!
- Permissionless P2P Networking
- PoW based consensus
- All-in-one implementation



https://medium.com/blockchannel/tools-and-technologies-in-the-ethereum-ecosystem-e5b7e5060eb9

Ethereum技术特点

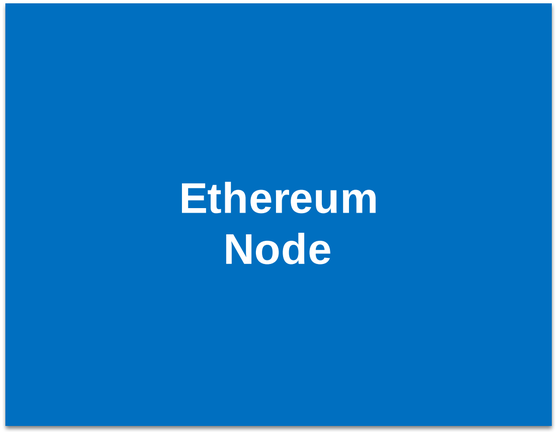
- It is (a) blockchain!
- Permissionless P2P Networking
- PoW based consensus
- All-in-one implementation



https://www.searchenginegenie.com/101-articles/Sybil-attack.html

Ethereum技术特点

- It is (a) blockchain!
- Permissionless P2P Networking
- PoW based consensus
- All-in-one implementation



Challenage to achieve consortium blockchain

Requirement for consortium blockchain

- Permissioned Network
- Data Privacy
- Flexible Consensus

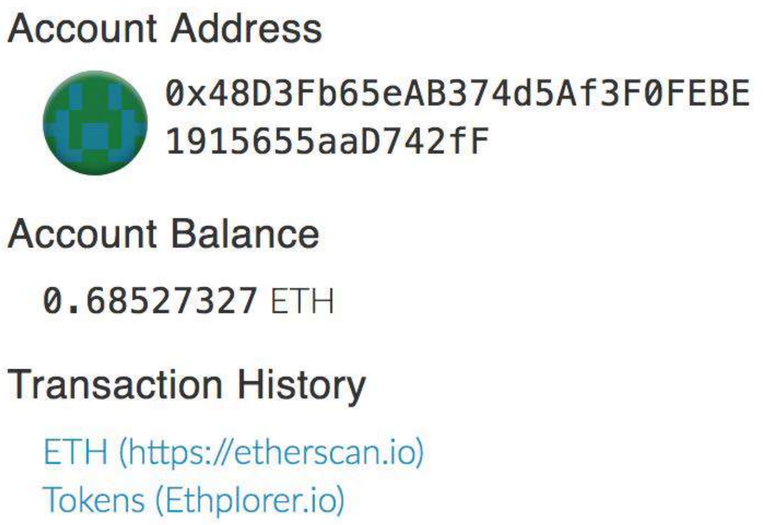
Permissioned Network

- Participant should be mapped to realworld identity
- Participant require permission to the network
- Exiting mechanism for retired participant

Permissioned Network

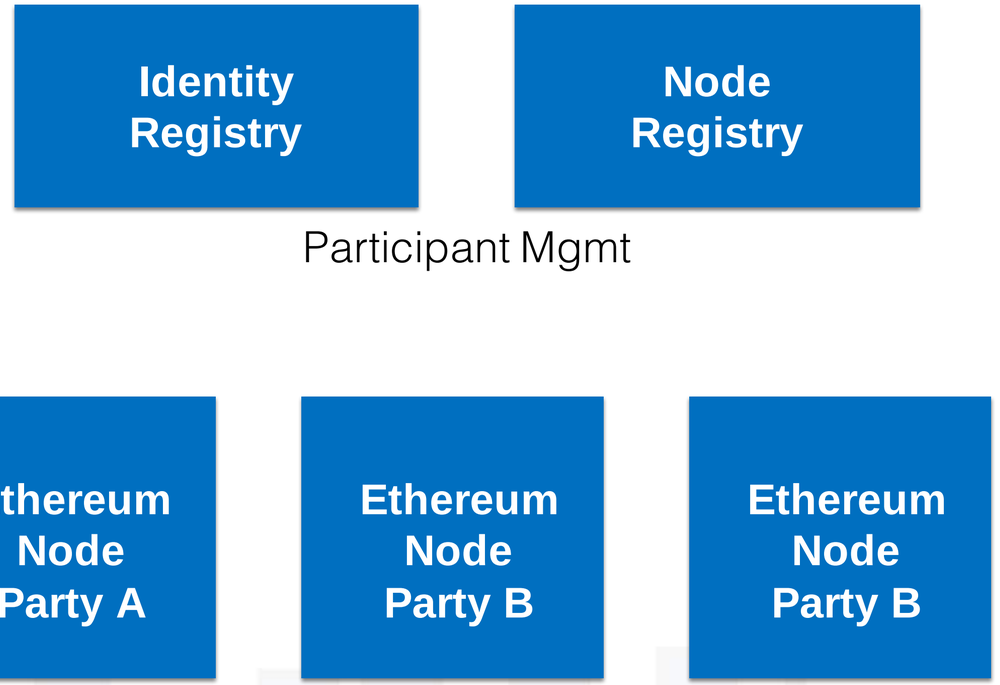
However in Ethereum

- Identity is anonymous and decentralized generated
- Node is decoupled from Identity and both of them could join network freely
- No retirement mechanism



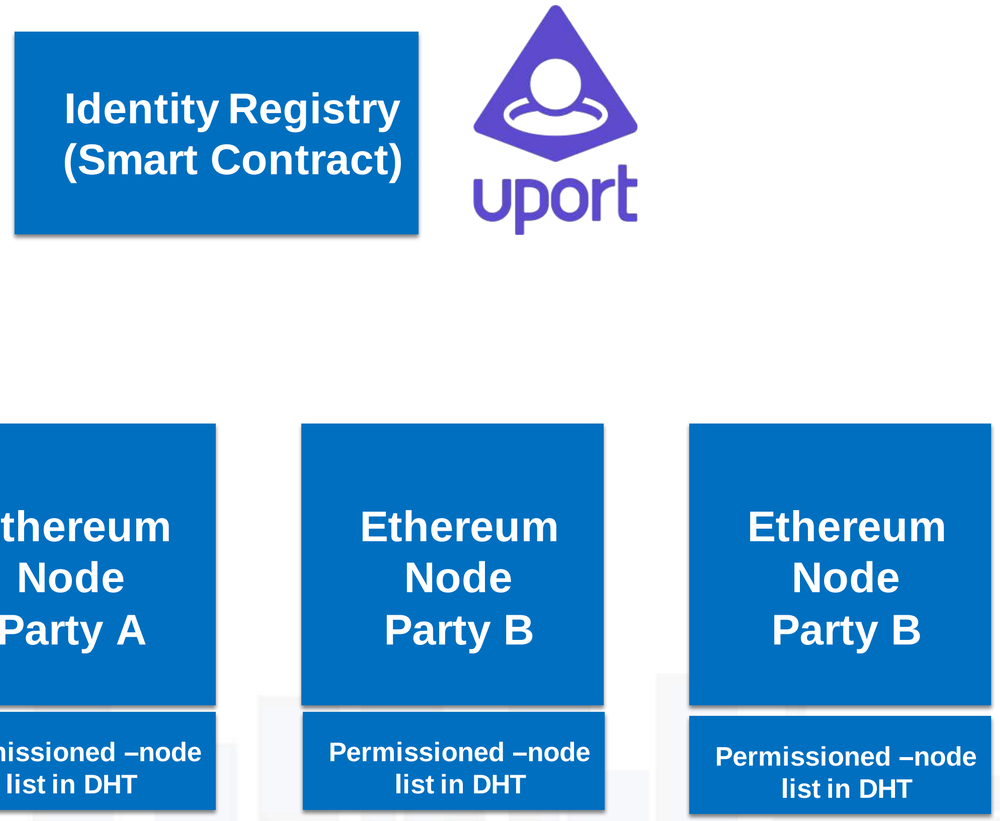
Permissioned Network: approach

- Manage Identity in a registry
- Binding node with an Identity
- Permissioned-nodes list to determine whom to connect with



Permissioned Network: approach

- Manage Identity in a registry
- Binding node with an Identity
- Permissioned-nodes list to determine whom to connect with



Data privacy

- Confidential ledger data should be visible by limited participants
- Transaction should be sent through limited participant

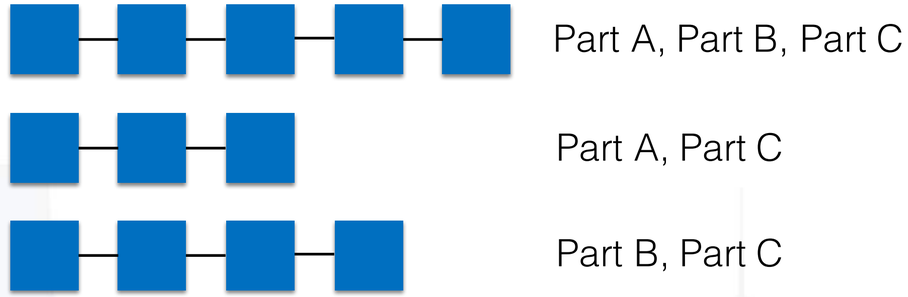
Data privacy

However in Ethereum

- Ledger data is open and transparant to all
- Transactions are sent to global network for consensus

Data privacy: approach

- Have multiple chains



Flexible Consensus

- No more PoW/PoS needed
- Higher performance and lower cost
- Alternative Consensus Mechanisms in different trust environment

How does consensus work, exactly?

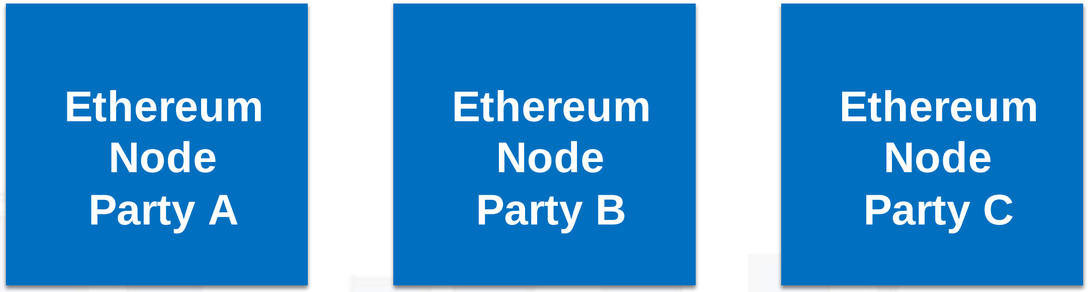
- Consensus on transaction order
- Consensus on transaction validataion

How does consensus work, exactly?

- Packing the transaction into block
- Compete for the proposer
- Choose the proposer
- Validate transaction and accept the block

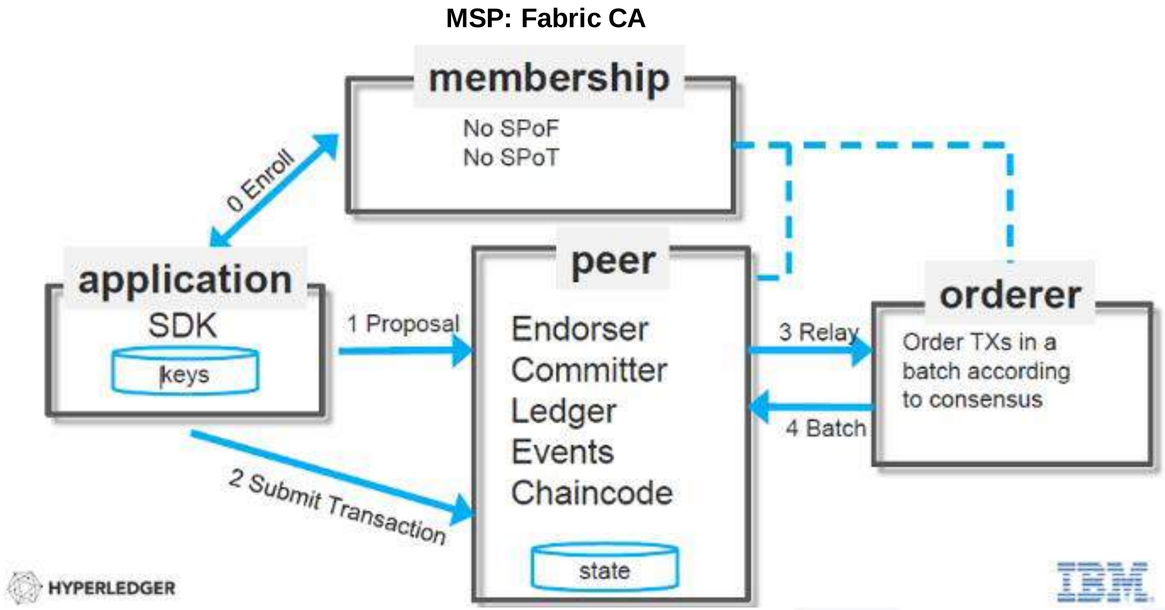
Flexible Consensus: approach

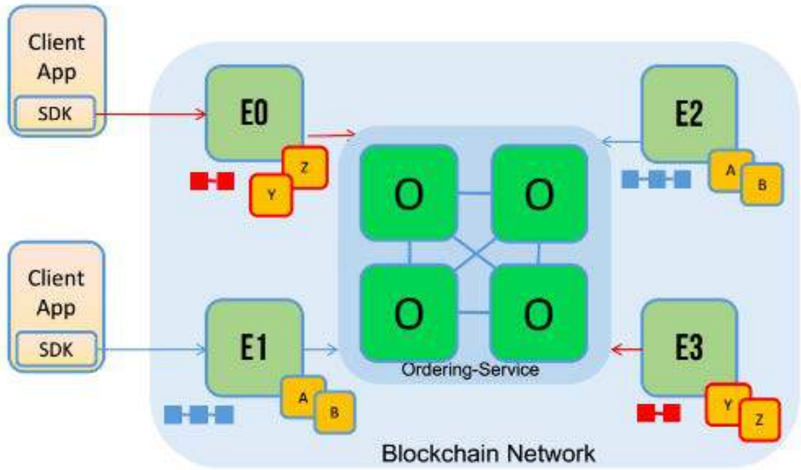
- Designate dedicated node as transaction packer



Real world consortium blockchain

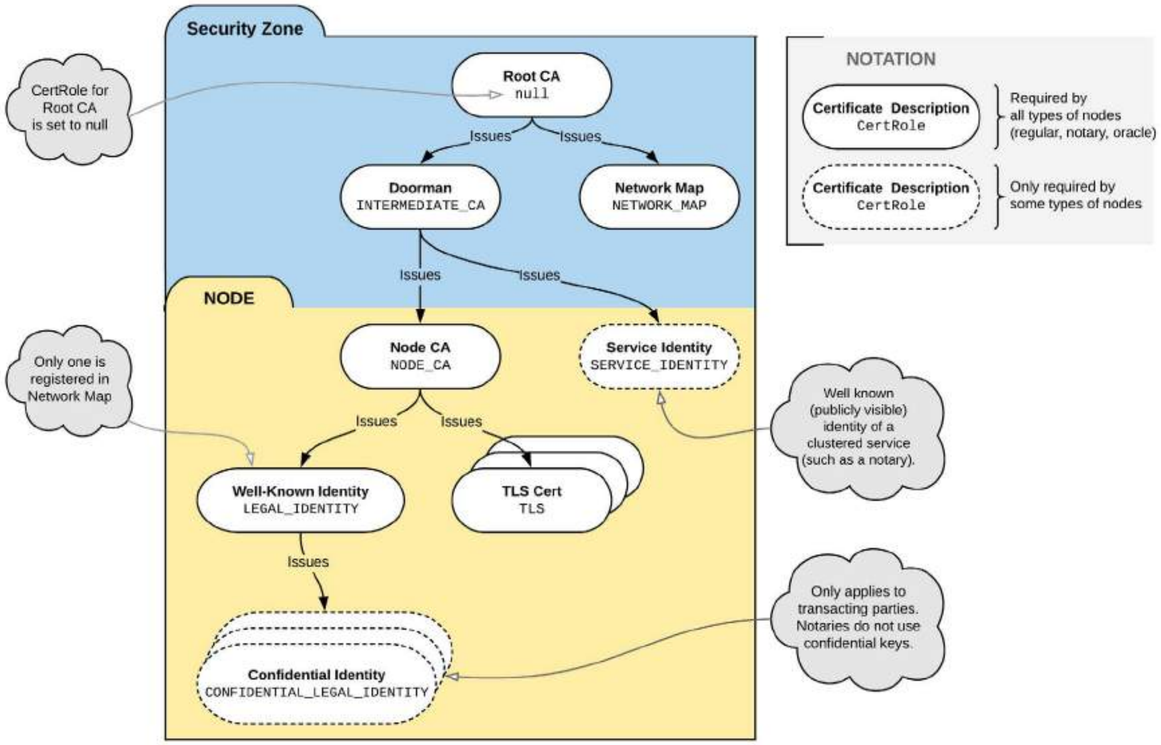
Hyperledger Fabric



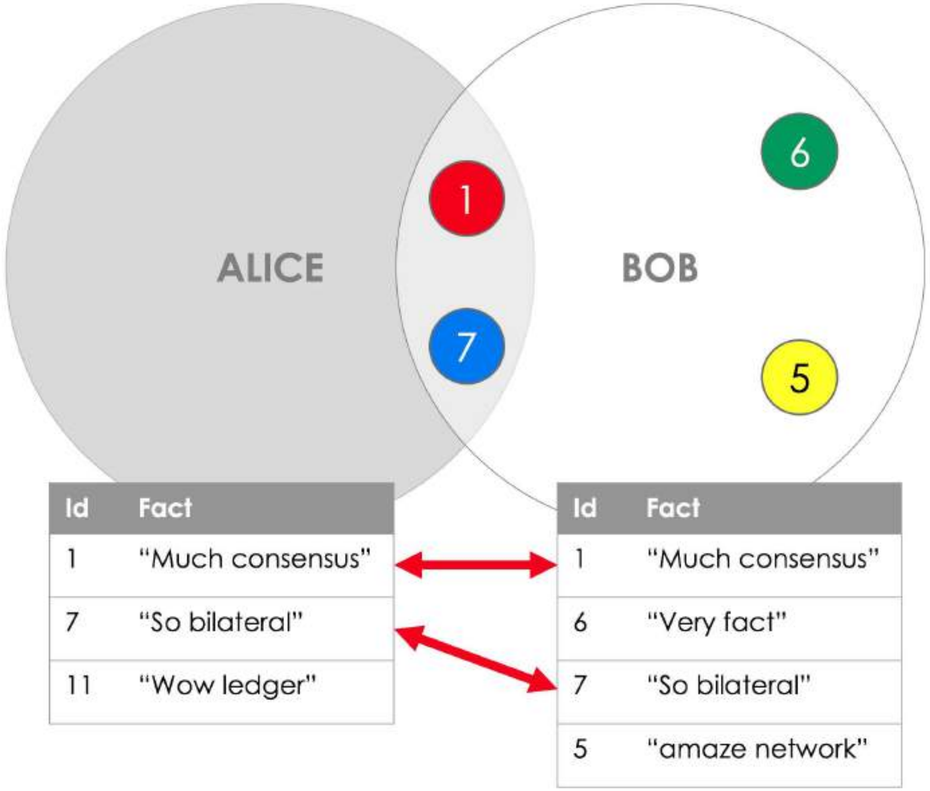


https://vitalflux.com/quick-glance-at-hyperledger-fabric-architecture/

Corda

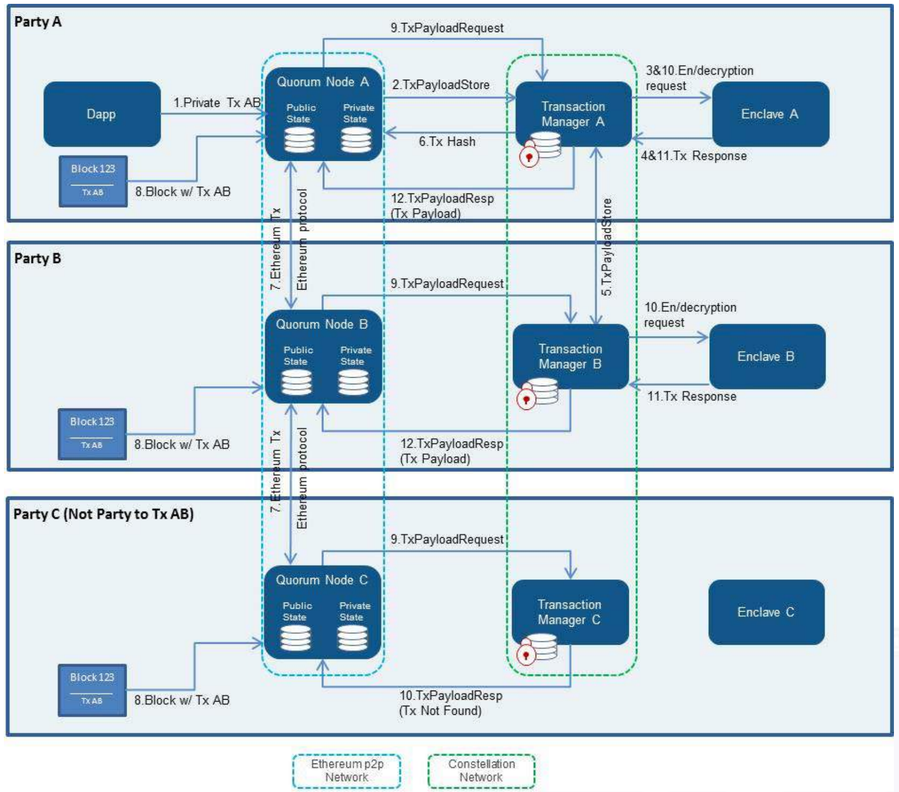


https://docs.corda.net/permissioning.html

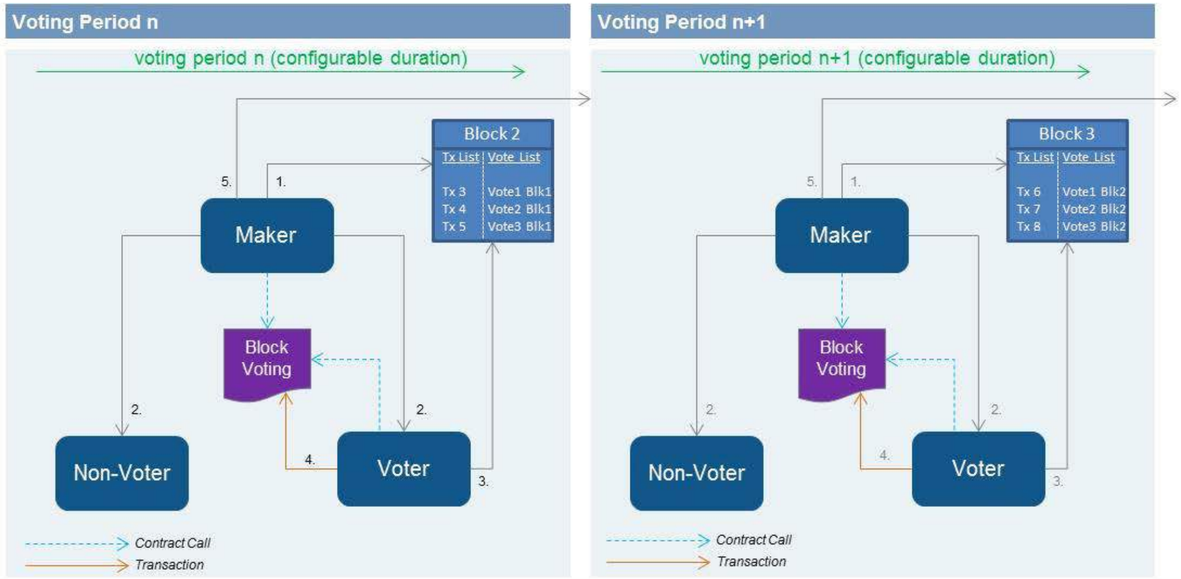


https://docs.corda.net/key-concepts-ledger.html

Quorum



https://github.com/jpmorganchase/quorum/wiki/Transaction-Processing



https://github.com/jpmorganchase/quorum/wiki/QuorumChain-Consensus

Patterns/Budilding Block for consortium blockchain

- Participant Mgmt Service
- Multiple chains/Ledger Segregation
- Designate dedicated node as transaction packer

主办方 Geekbang. 极客邦科技 InfoQ

GMTC 2018

全球大前端技术大会

大前端的下一站

<<扫码了解更多详情>>

极客邦科技
企业培训与咨询

Geekbang.

扫码关注

获取更多培训信息