本体区块链实践

从分布式到去中心化

胡凝

ONTology

自我介绍

胡凝

- Ontology 协议架构专家

议题

- 区块链共识
- 本体区块链体系
- 本体应用

区块链共识

区块链 与 共识

- 为什么要共识?
  - 定义交易的执行顺序
  - 为交易处理结果的一致性提供基础
- 区块链的共识算法定义了链的架构 / 适用场景

- 共识的选择
  - 取决于参与方的规模
  - 取决于参与方的关系也决定了链的组成方式
  - 取决于链的运营方式
  - 取决于对网络交易性能的需求
  - 取决于对参与方的激励设计

区块链共识算法

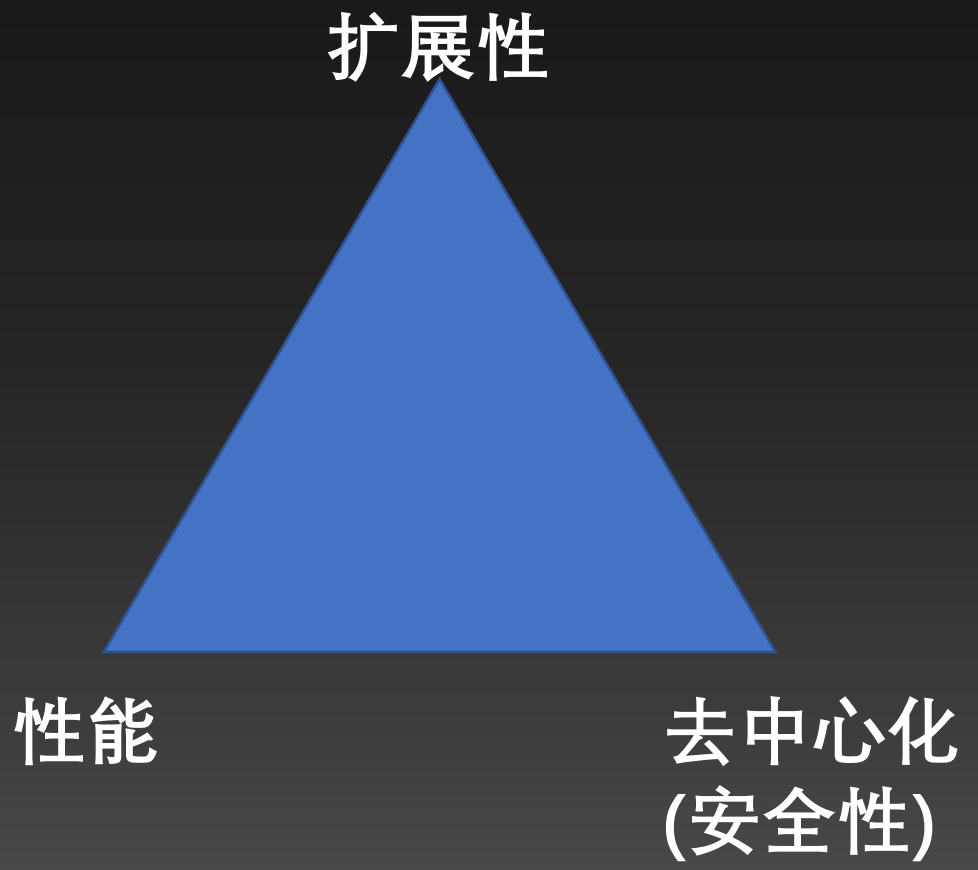
- 基本要求
  - 一致性 （safety）
  - 终局性（liveness）
  - 容错（fault tolerance）
- 扩展要求
  - 去中心化
  - 扩展性
  - 性能（message complexity）
  - 追责（accountability）
  - ~~运维~~ => 治理（governance）
  - 动态参与

共识算法（共识协议）

- 一致性（safety）
  - 所有参与共识的诚实的节点，得到的计算结果是相同的，而且是符合共识协议的。
- 终局性（liveness）
  - 所有参与共识的诚实的节点，最终可以达成一致性结果
- 容错性
  - 在共识算法的成功执行过程中，可以容许参与共识的节点发生那些错误
    - 失败节点立即停止 (Crash Stop)
    - 拜占庭容错 (Arbitrary Action)

共识算法

- 扩展要求
  - 去中心化
  - 扩展性
  - 性能（message complexity）
  - 追责（accountability）
  - 治理（governance）
  - 动态参与



分布式系统模型

- 同步模型
  - 节点间消息传递有时间上限，而且上限已知
- 异步模型
  - 节点间消息可以确保传递成功，但是时间上限未知，节点处理消息时间未知
- 弱同步模型
  - 节点间消息传递和处理有时间上限，但是上限未知

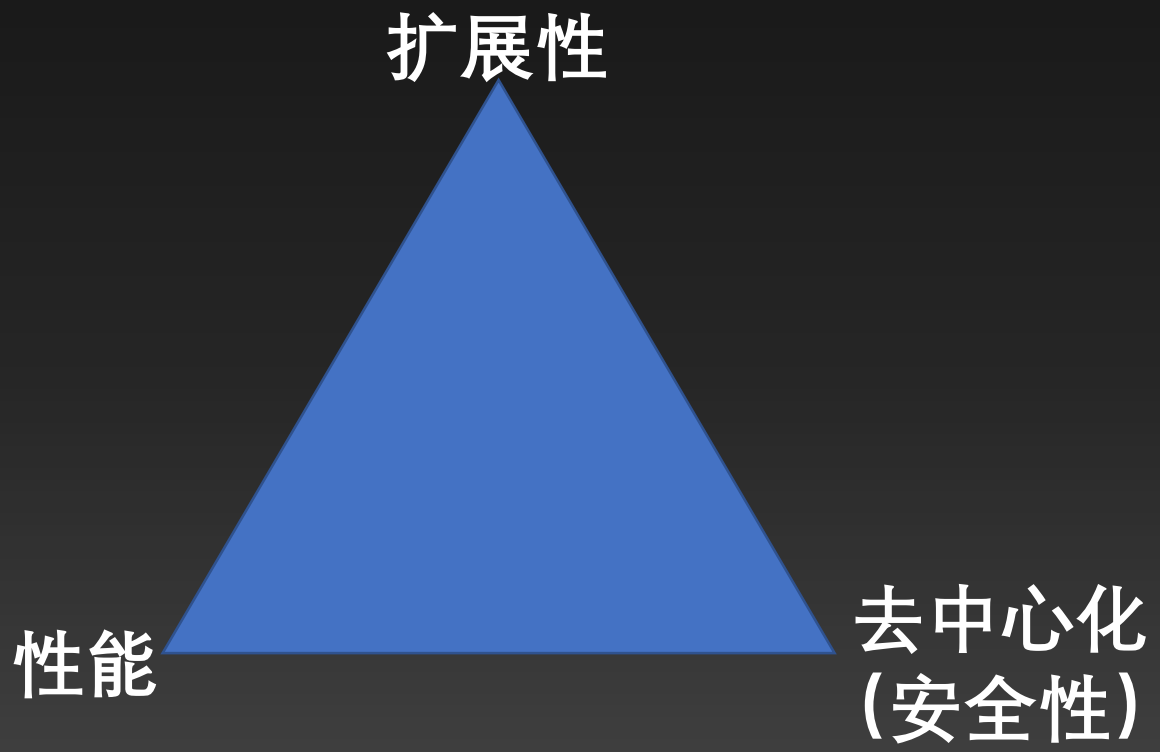
- FLP(Fisher-Lynch-Patterson-1985) says no asynchronous consensus algorithm can guarantee both safety and liveness.

当前主流的共识算法

- 基于链的共识算法
  - 比特币 (工作量证明 Proof-of-Work)
  - 以太坊 (权益证明 Proof-of-Stake)
  - DAG
- 基于拜占庭容错的共识算法
  - Tendermint
  - Algorand
  - Ontology VBFT
- 面向场景的共识算法
  - Hyperledger Fabric Orderer

共识与区块链应用场景

- 区块链应用 之 公有链
  - 基于公有链通证机制引入激励
  - 去中心化程度高
  - 完全开放式应用
- 区块链应用 之 联盟链
  - 基于区块链构建行业联盟
  - 许可式应用
  - 可定制链下容错方案



公有链系统的容错要求

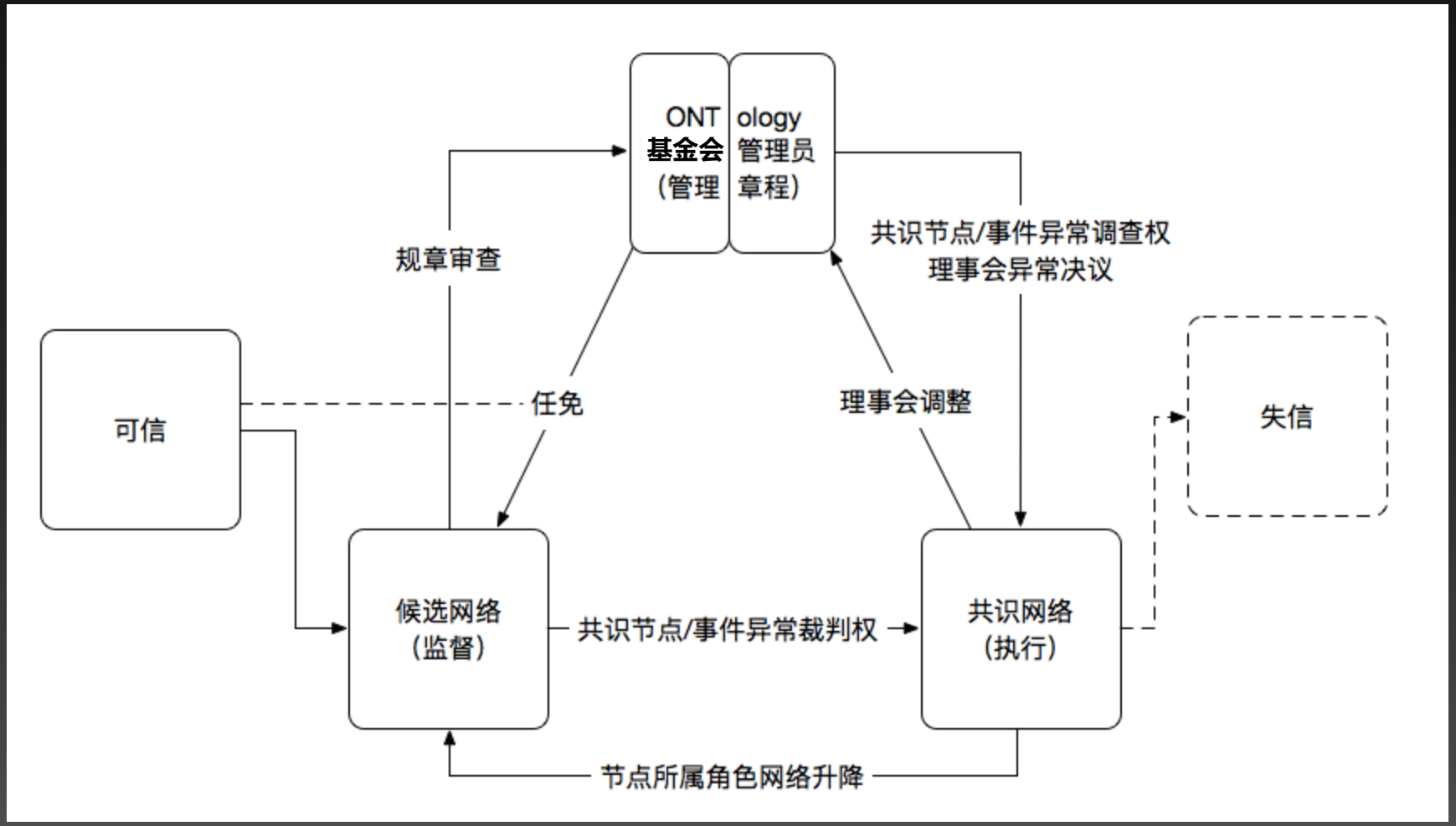
- System Crash
- Sybil Attack
  - 多重身份 / 伪造身份攻击
- 51% equivalent attack
  - 二义性行为攻击，致使多种路径都达到majority
- Long Range Revisions
  - 在历史区块上通过51%攻击造成分叉
- Nothing at stake
  - 多个fork上进行无差别投票，从而使区块无法终局
- Bribing attack
  - 集体贿赂投票，从而使权益证明失去公平性

本体区块链体系

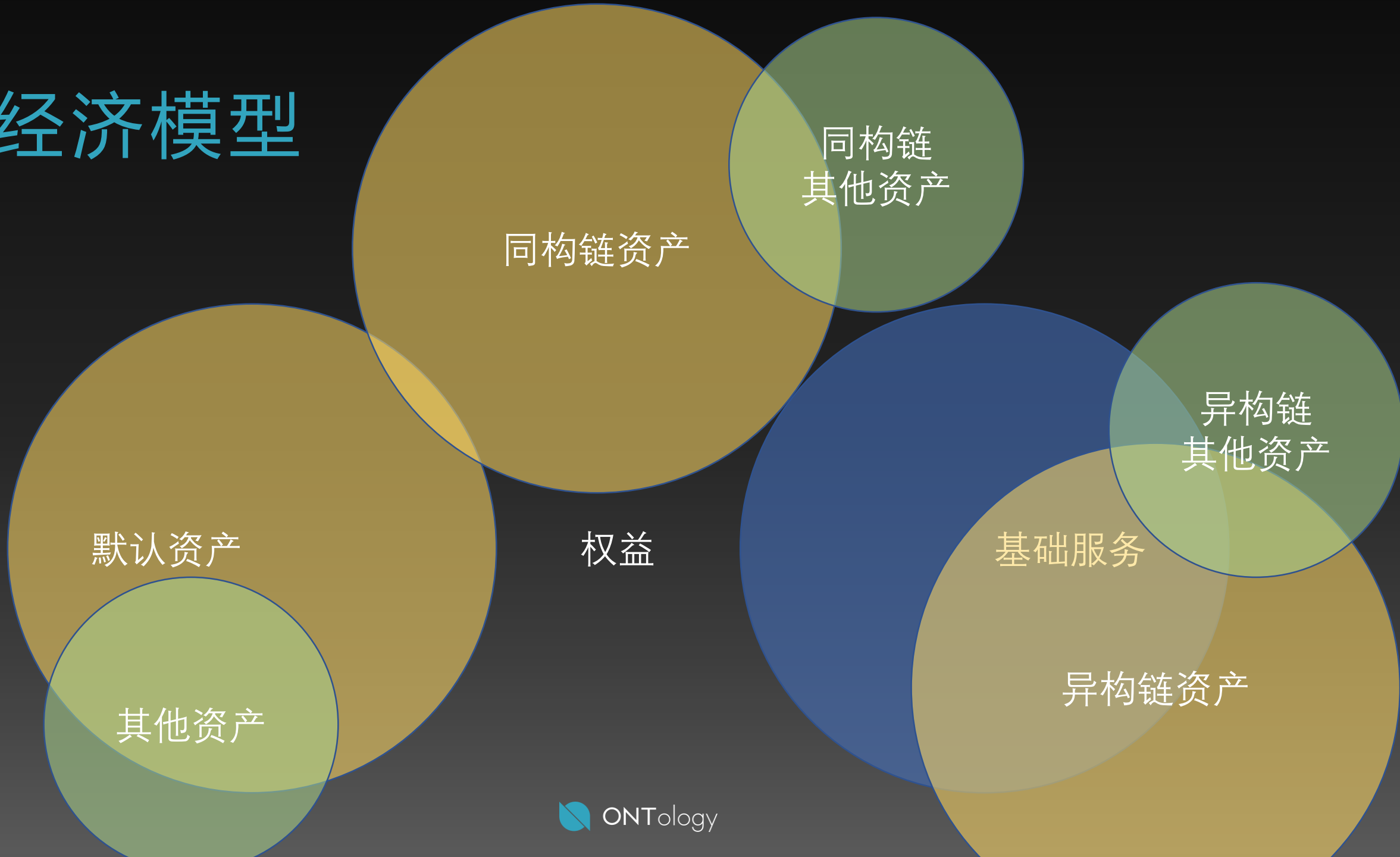

治理
经济
组网
共识

治理模型

- 治理假设
- 链上治理
- 链网治理
- 链外治理

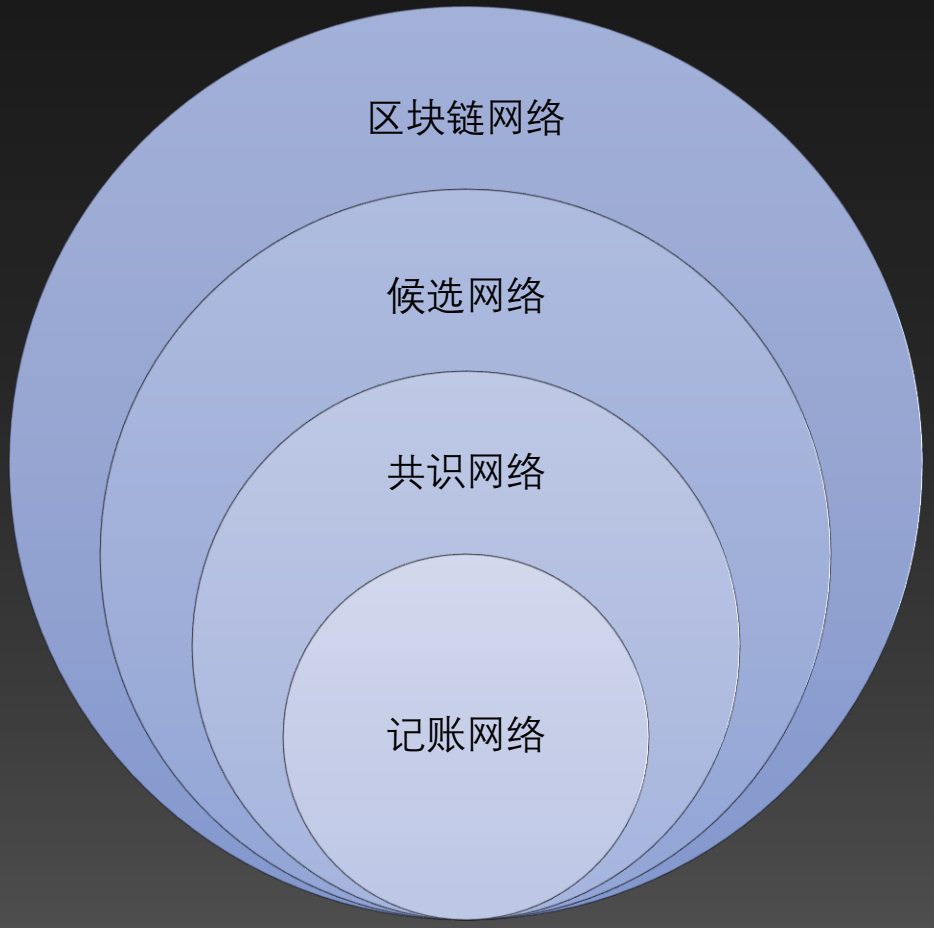


经济模型



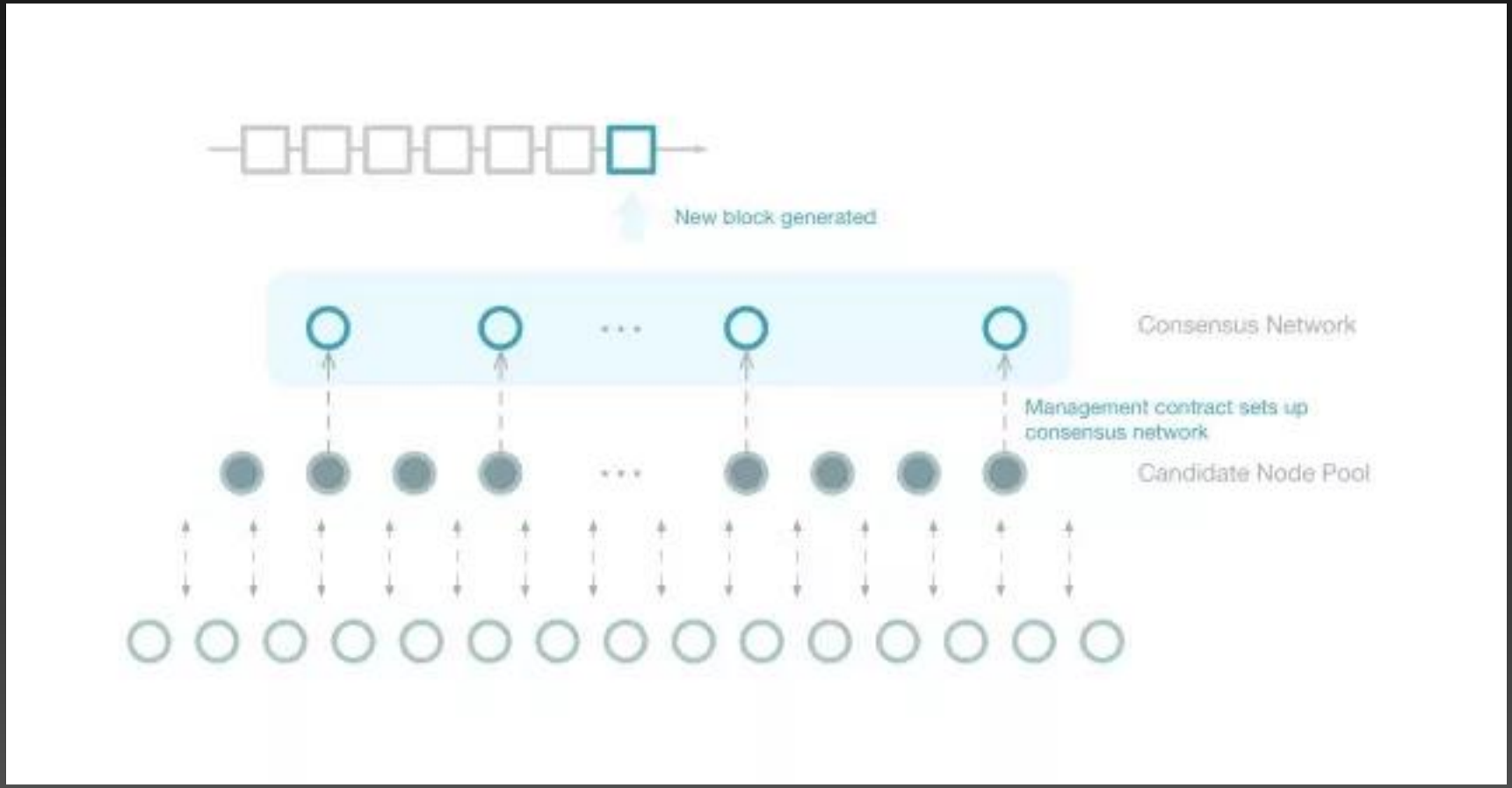
ONTology

组网模式



ONTology

Ontology网络架构



VBFT共识设计

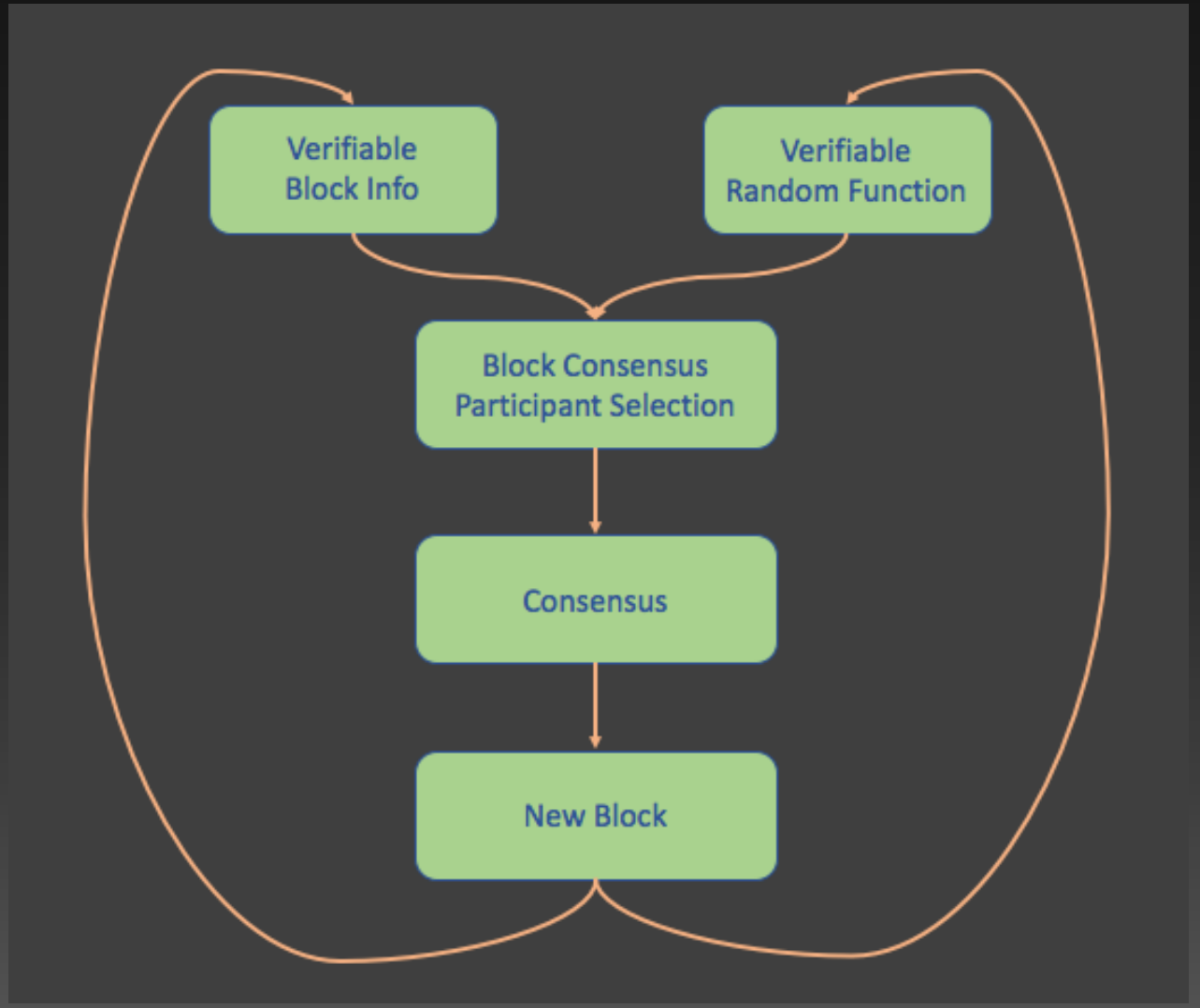
- **支持共识群体的规模性扩展**
- 保障共识群体生成的随机性和公平性

- 快速地达到状态终局性

ONTology

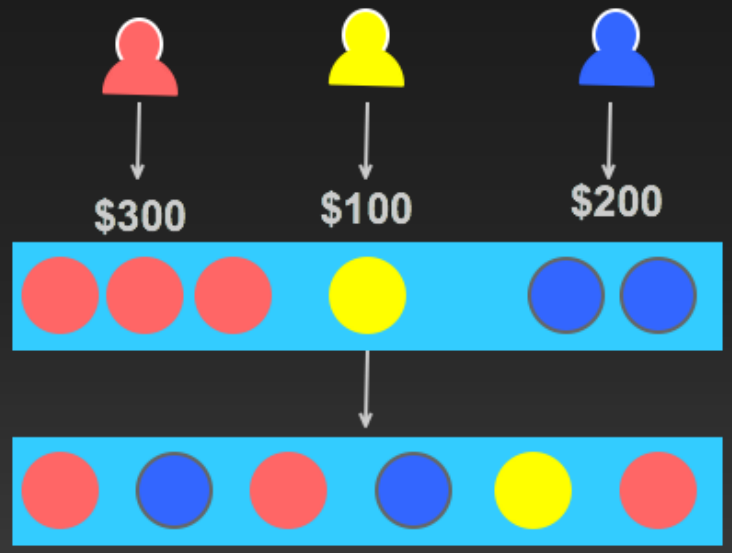
VRF (Verifiable Random Function)

- 可验证随机函数
  - result = VRF_Hash（SK，info）
- 基于前一个区块的VRF生成
- VRF + PeerStakeTable
  - 基于Stake的节点随机选取



PoS

- 基于PoS，随机确认共识节点的角色
- 共识治理
  - 每个节点的信息｛PeerID，Peer-PublicKey, Stake}
  - 按照每个节点的 Stake 组建共识网络
- PeerStakeTable
  - 随机打散的Peer节点表，
  - 节点在表中的项数正比于 节点的Stake
  - 通过VRF + PeerStakeTable，确认节点角色

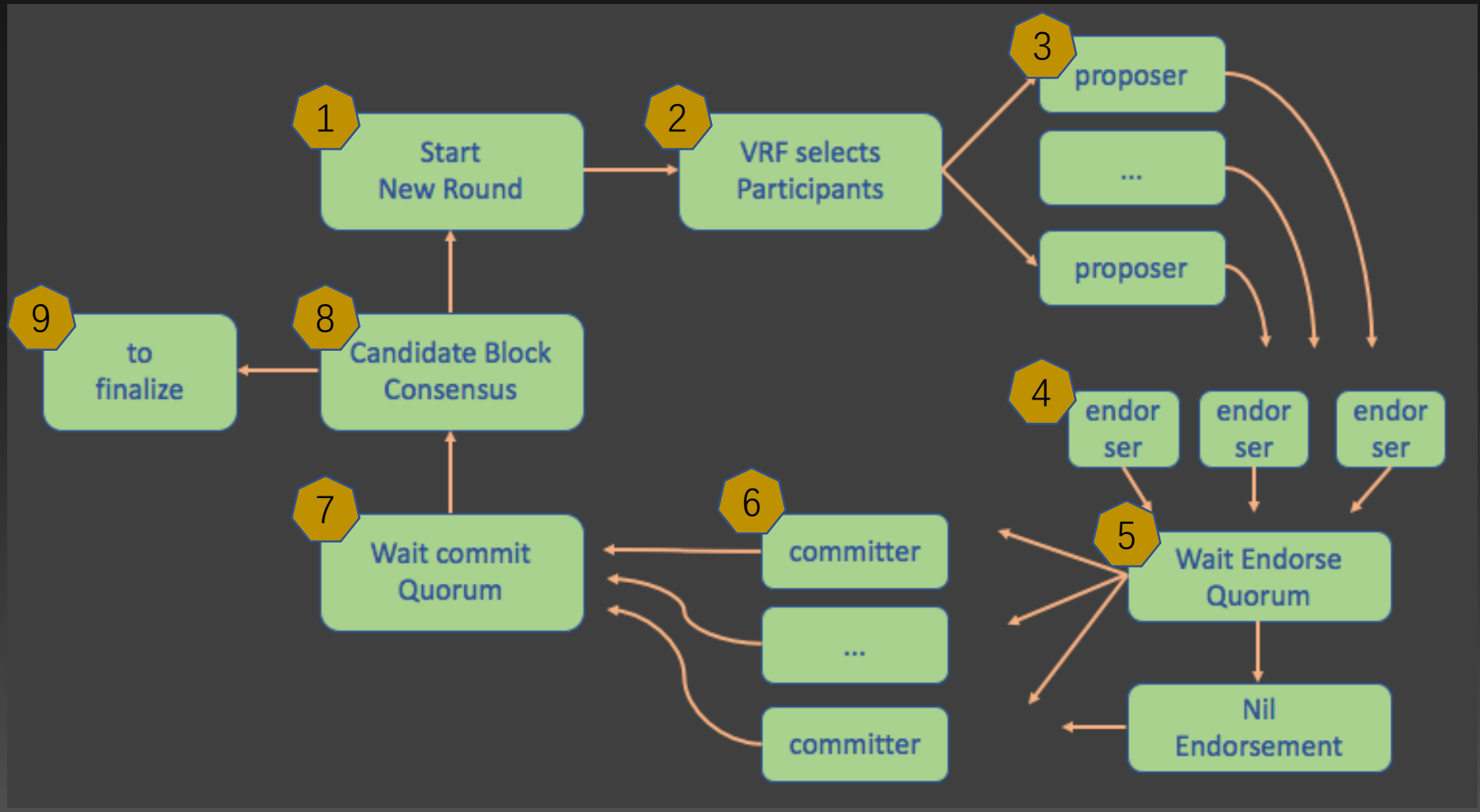


VBFT

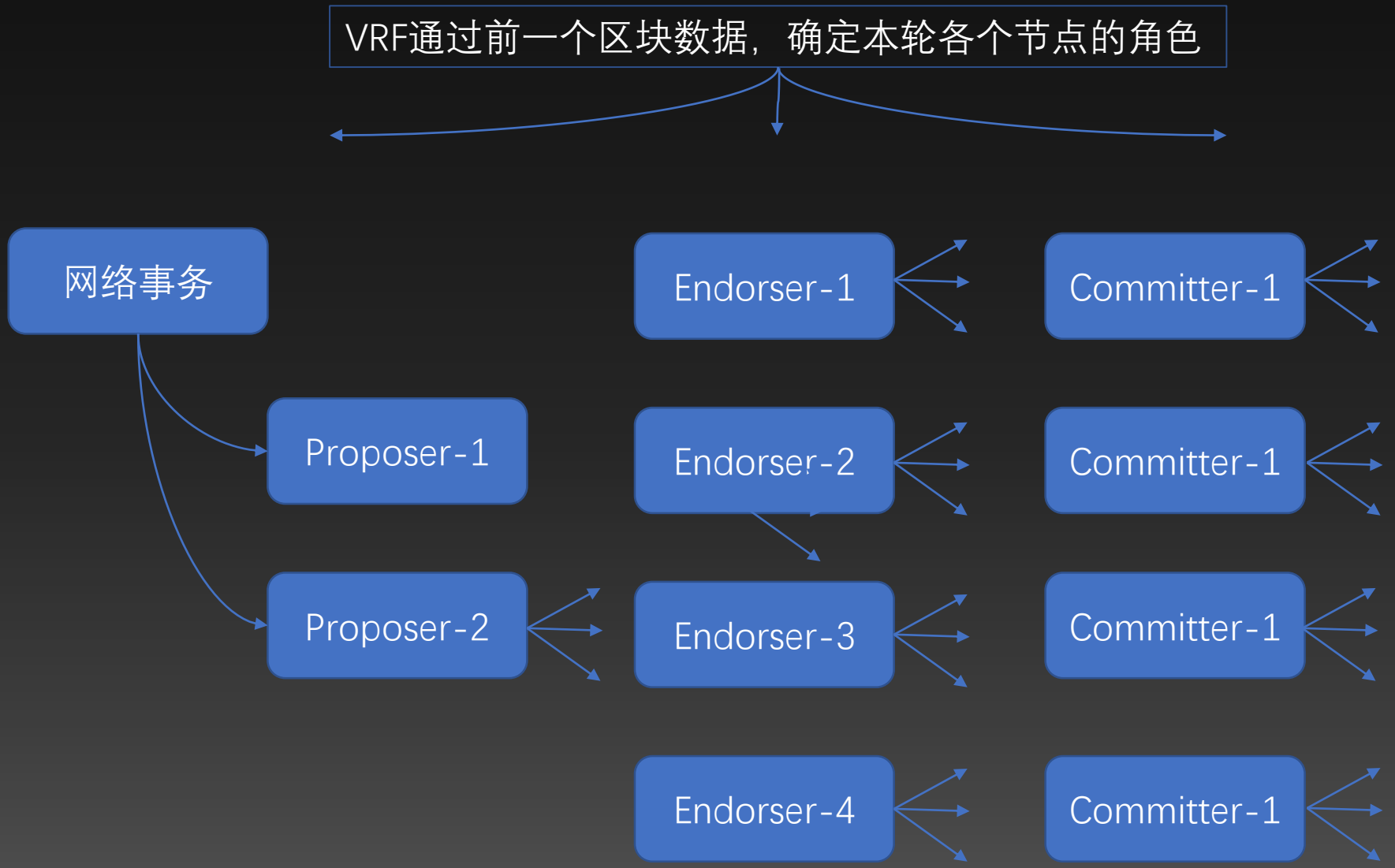
- VBFT治理合约根据PoS，选择共识节点集合
- 共识节点在一个epoch内负责网络中所有区块的共识

  - 启动一个区块高度的共识
  - 通过VRF，确认集合中各个共识节点的角色
  - proposer提出区块
  - endorser验证区块
  - committer确认区块
  - 完成一个共识

VBFT



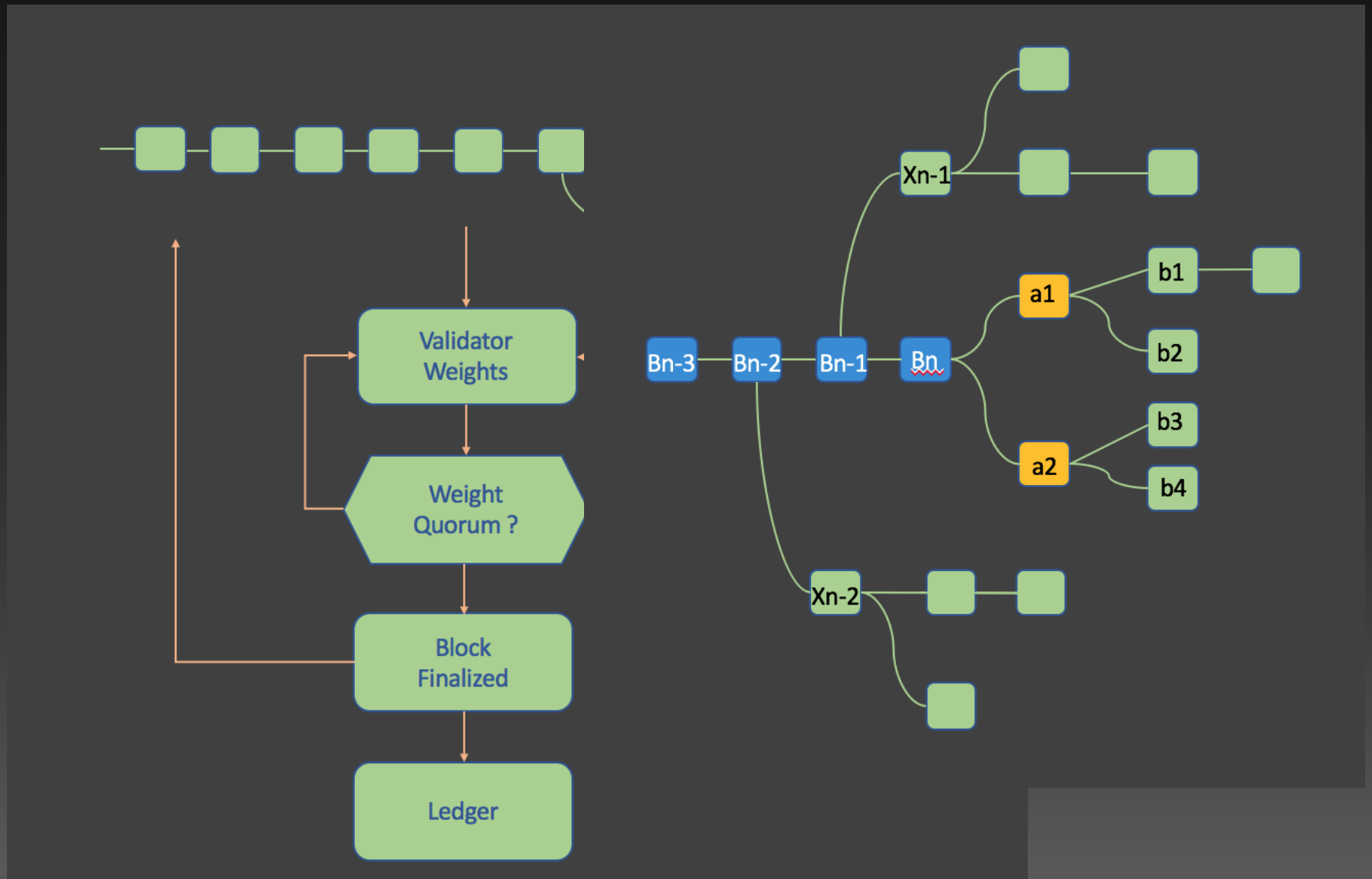
ONTology


VRF通过前一个区块数据，确定本轮各个节点的角色
网络事务
Proposer-1
Proposer-2
Endorser-1
Endorser-2
Endorser-3
Endorser-4
Committer-1
Committer-1
Committer-1
Committer-1

ONTology

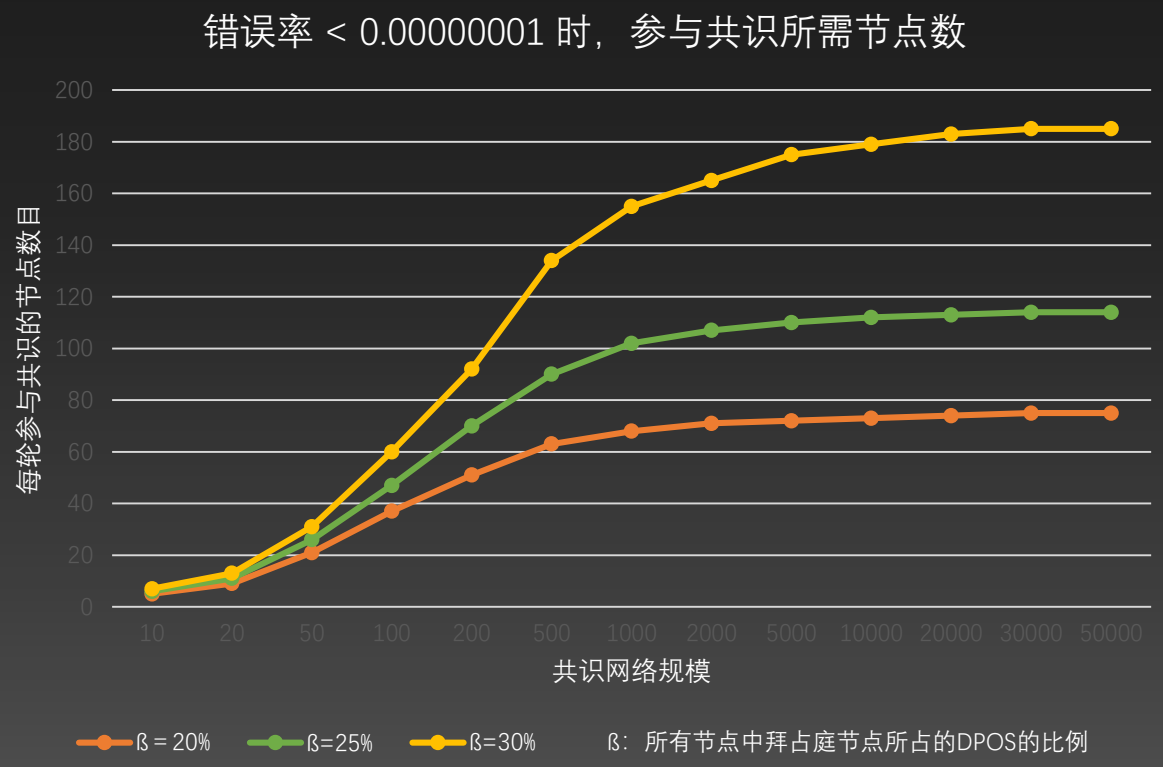
VBFT 终局性

- 基于PoS实现终局性



VBFT的扩展性

- 通过VRF随机挑选节点，减少共识节点参数数目同时提高共识效率



ONTology

VBFT的治理

- 治理机制
  - 节点管理
  - 共识节点的选举与更新
- 激励机制
  - 网络节点收益的分配
- 惩罚机制

- 基于智能合约实现治理
  - 网络节点的生命周期
  - 网络节点的抵押权益
  - 网络交易手续费
  - 网络节点的容错与惩罚机制

本体区块链解决方案

ONTology

Ontology Blockchain(本体)

- **https://github.com/ontio/ontology**
- 本体区块链框架
  - 微服务化架构
  - 分布式账本
  - P2P网络协议
  - 模块化的共识协议
  - NeoVM智能合约平台

- 一条或多条提供基础性通用服务的公有链
  - 实体映射
  - 进行数据交换通用协议支持
  - 提供通用性智能合约服务体系

- 各个行业、地域和不同的业务场景，可以有自己独有的业务链

设计原则

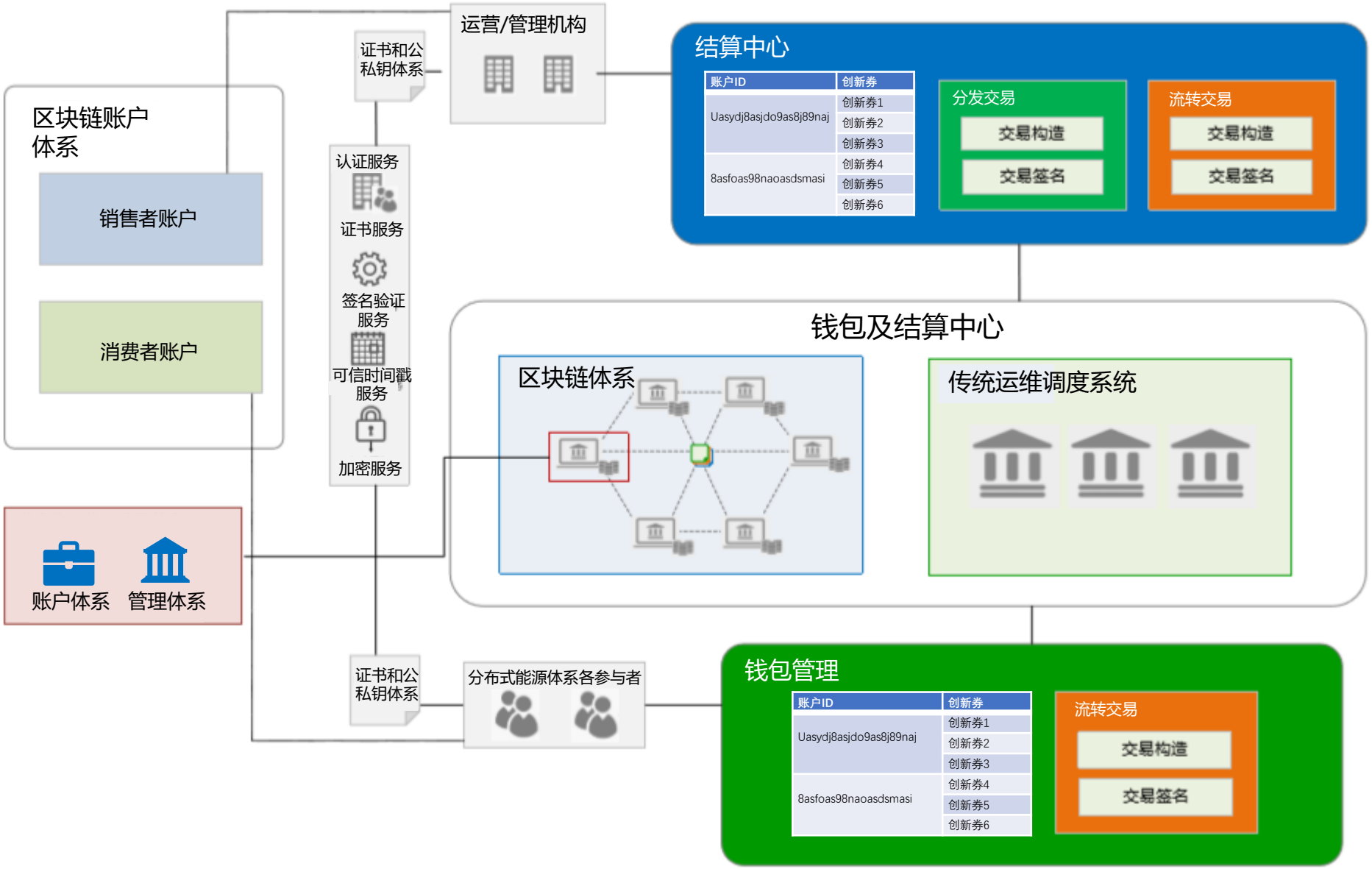
- **定律一，“不要拿大炮打蚊子”**，区块链技术更适宜于资产网络（Assets Over IP）

- **定律二，使用区块链，一定是要有多方写入数据的需求**

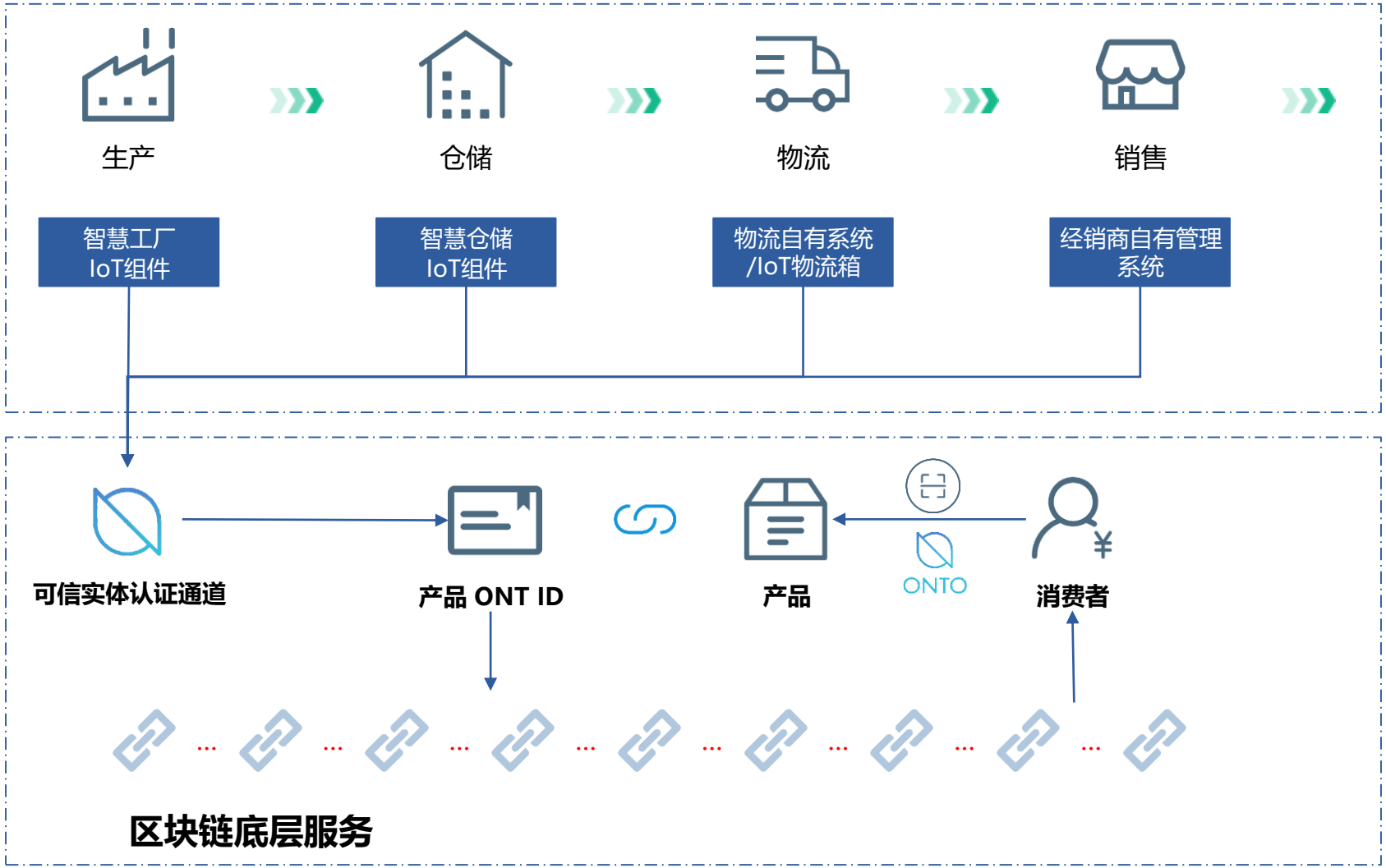
- **定律三，区块链产品一定是天然的弱中心化的**

——段新星《钛坦白》

结算中心


运营/管理机构
证书和公私钥体系
结算中心
账户ID
创新券
Uasydj8asjdo9as8j89naj
创新券1
创新券2
创新券3
8asfoas98naoasdsmasi
创新券4
创新券5
创新券6
分发交易
交易构造
交易签名
流转交易
交易构造
交易签名
区块链账户体系
销售者账户
消费者账户
认证服务
证书服务
签名验证服务
可信时间戳服务
加密服务
钱包及结算中心
区块链体系
传统运维调度系统
账户体系
管理体系
证书和公私钥体系
分布式能源体系各参与者
钱包管理
账户ID
创新券
Uasydj8asjdo9as8j89naj
创新券1
创新券2
创新券3
8asfoas98naoasdsmasi
创新券4
创新券5
创新券6
流转交易
交易构造
交易签名

供应链物料&信息管理



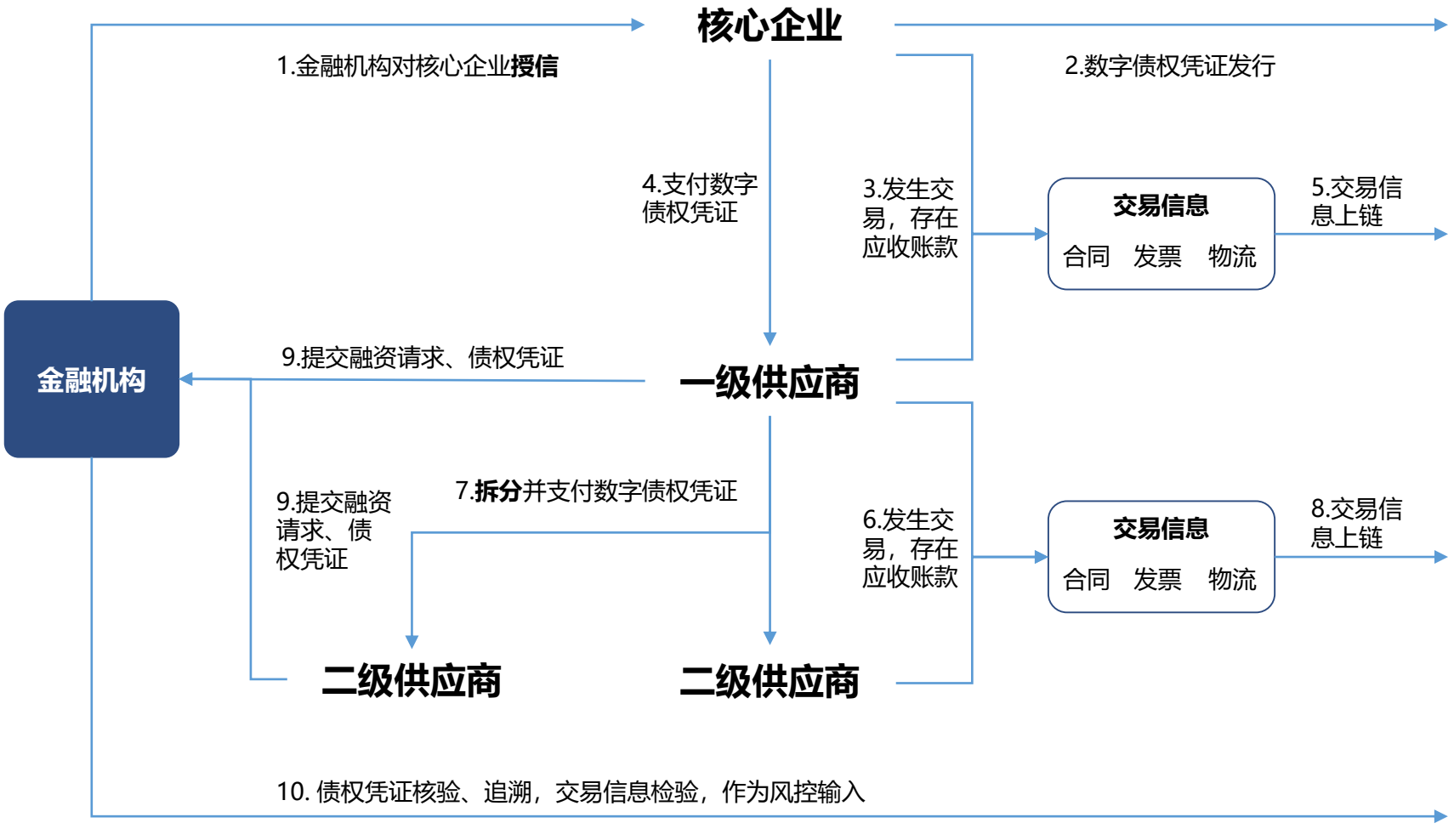
物料管理部分：

- 产能、仓储周期、物流周期、销售周期
- 供货量，地域分片，窜货管理
- 需求量分析，跨地域调度策略

信息管理部分：

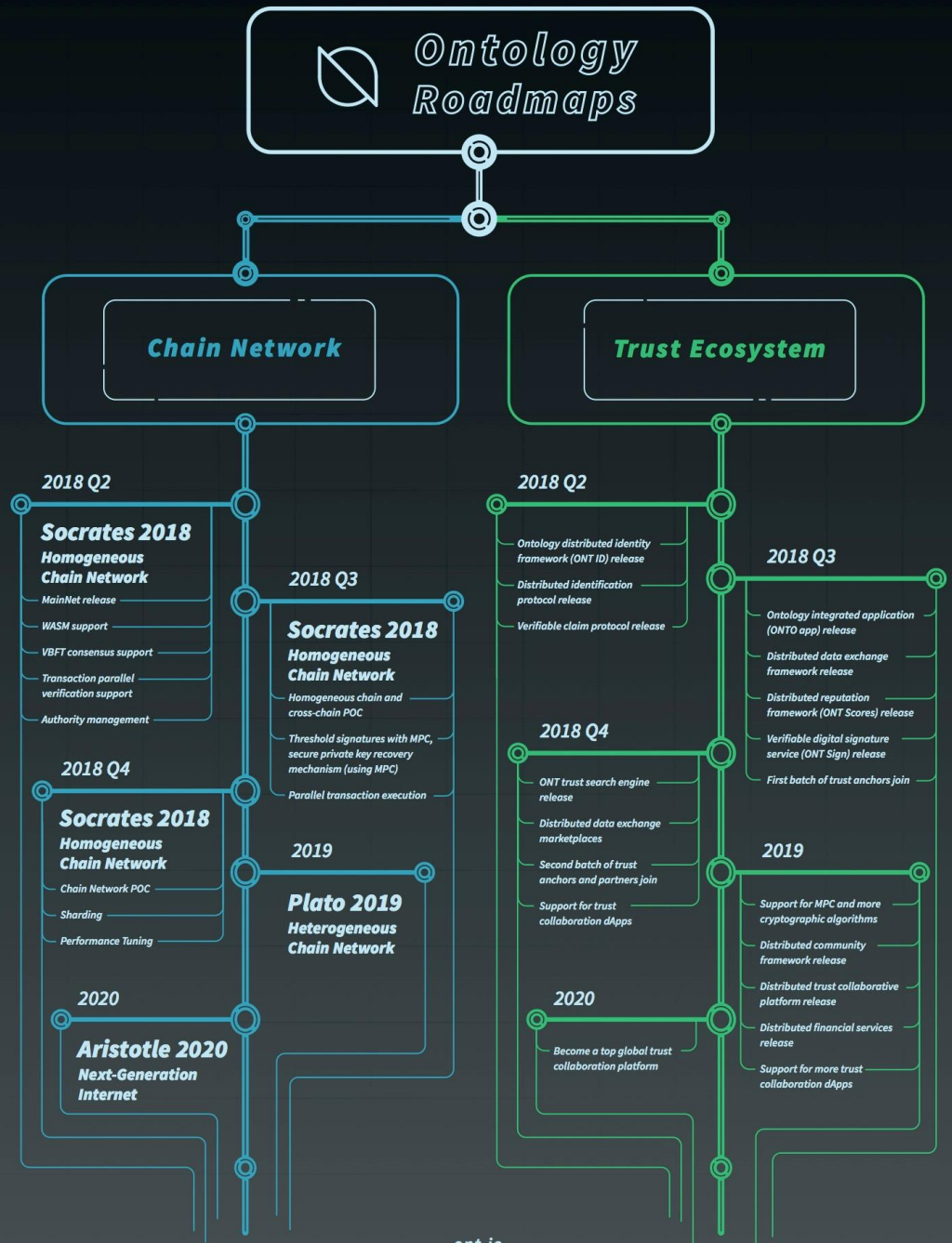
- 链条关键节点数据上链，出厂信息、仓储信息、物流信息、销售情况
- 通过可信实体认证通道，建立产品可信身份，链接实体产品，传达信息到消费者

供应链资金管理



- 核心企业以其应收账款为底层资产，发行数字化债权凭证，支付下游企业，并作为其融资依据。
- 金融机构与核心企业也可以基于区块链提供的真实数据进行供应商管理。

本体计划



ont.io

Ontology
本 体

BCCon
全球区块链生态
技术大会

https://ont.io/

ONTology