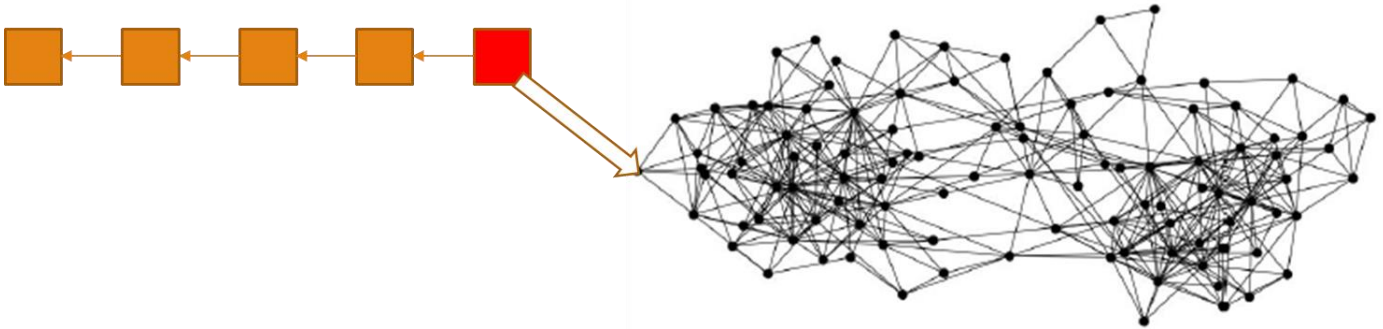
共识协议与区块链系统

范磊

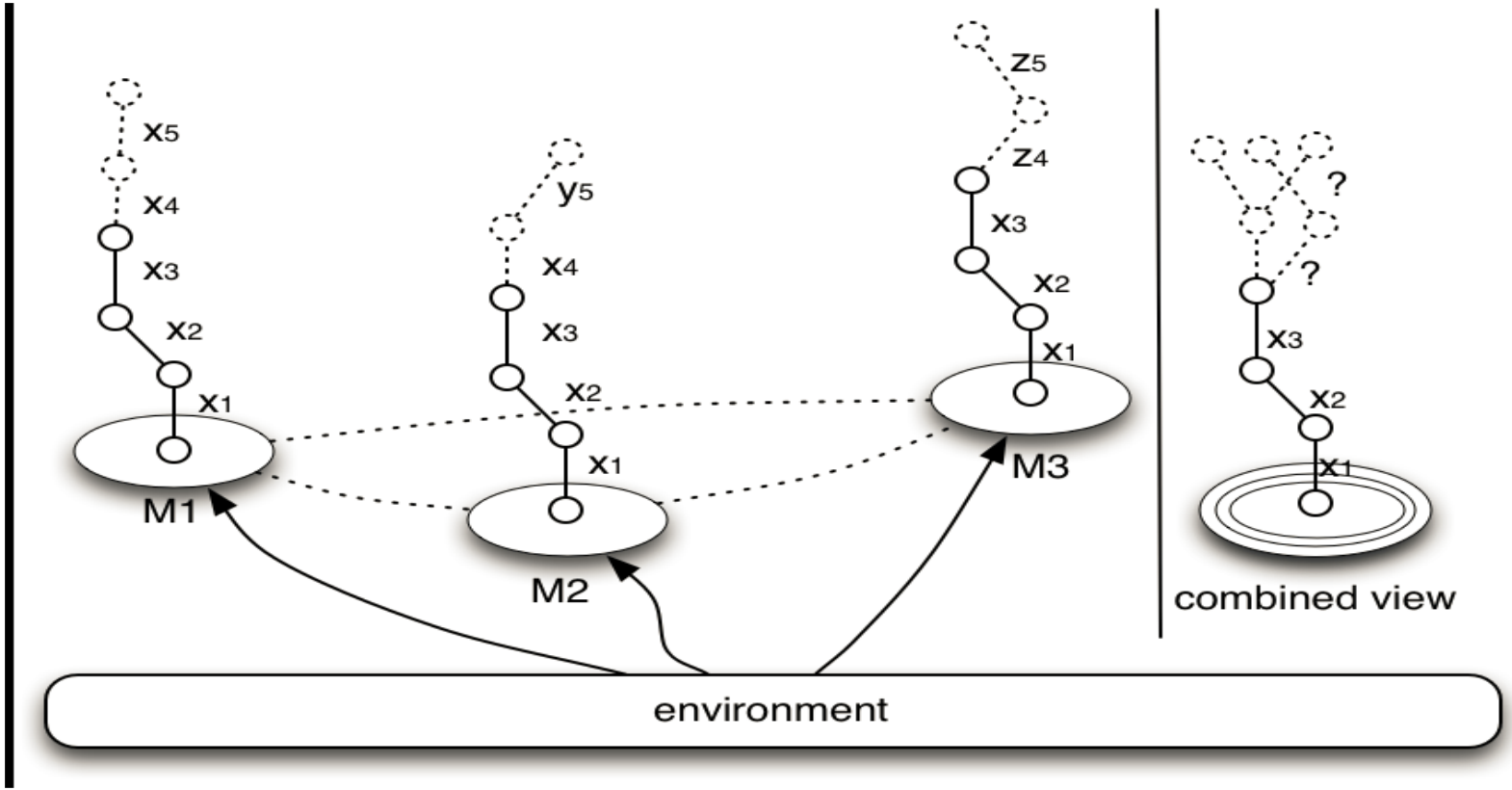
上海交通大学

区块链网络的组织方式

- 比特币及区块链使用基于P2P网络的广播通信，新生产区块以及交易数据通过节点间的泛洪传递到所有节点
  - 信息从最近的邻居节点开始，通过多跳传递到全部网络
  - 各个节点接收信息可能延迟、错序以及丢失部分信息



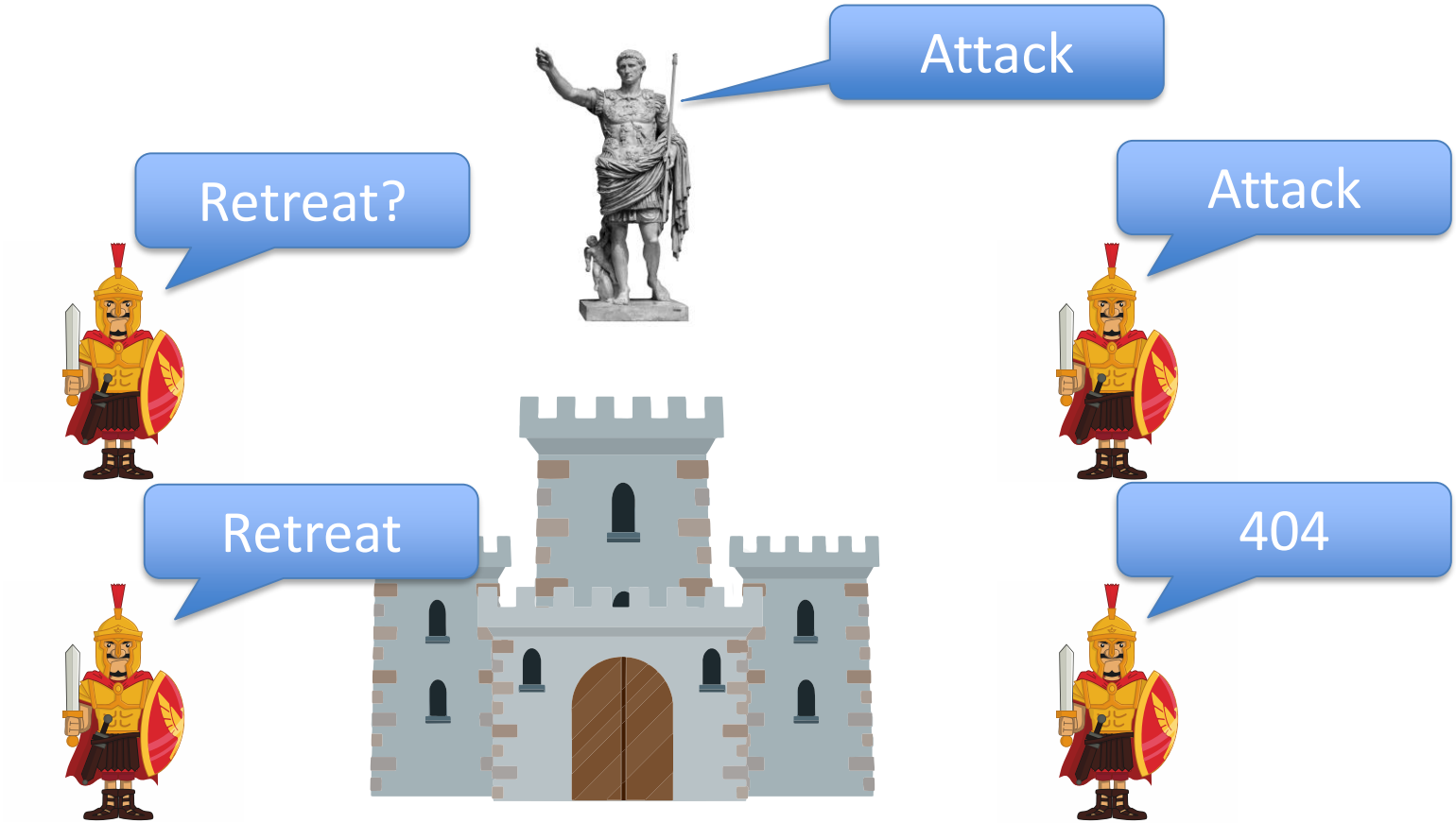
区块链系统的全局模型


x5
x4
x3
x2
x1
M1
y5
x4
x3
x2
x1
M2
z5
z4
x3
x2
x1
M3
?
?
x3
x2
x1
combined view
environment

共识问题（Consensus）

- 计算机领域的经典问题
  - 多个参与节点（可能有恶意节点），各自产生输出，共识协议应满足：
    - 一致性，所有诚实节点应有相同的输出
    - 有效性，如果诚实节点的输入相同，则输出应保持不变
    - 终止性，共识过程应能够在相应的时间内结束
- [Pease，Shostak，Lamport 1980]提出，当且仅当节点数量满足$n \geq 3m + 1$时，诚实节点可以达成共识
- [Lamport，Shostak， Pease 1982]提出著名的拜占庭将军问题
- [Fischer，Lynch，Paterson 1985]提出，在异步网络中，如果有哪怕一个失效节点，诚实节点不可能确定性达成共识

拜占庭将军问题

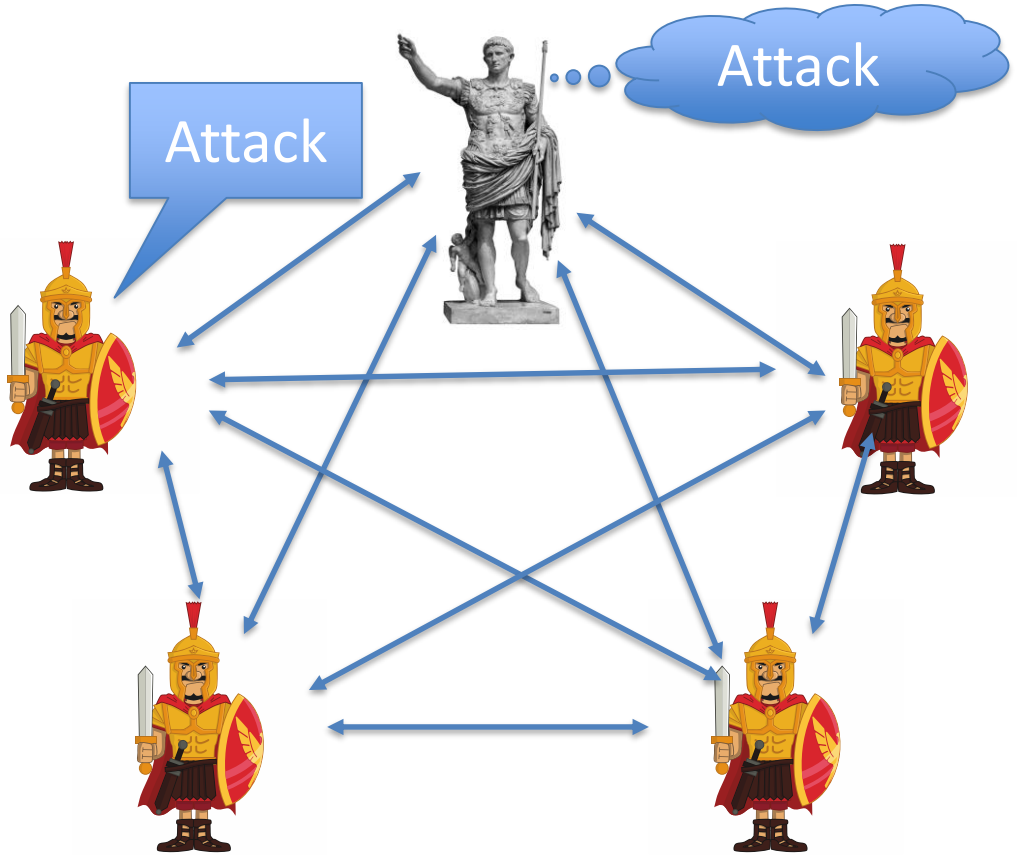


拜占庭将军问题

首领节点(Leader)输入 0/1

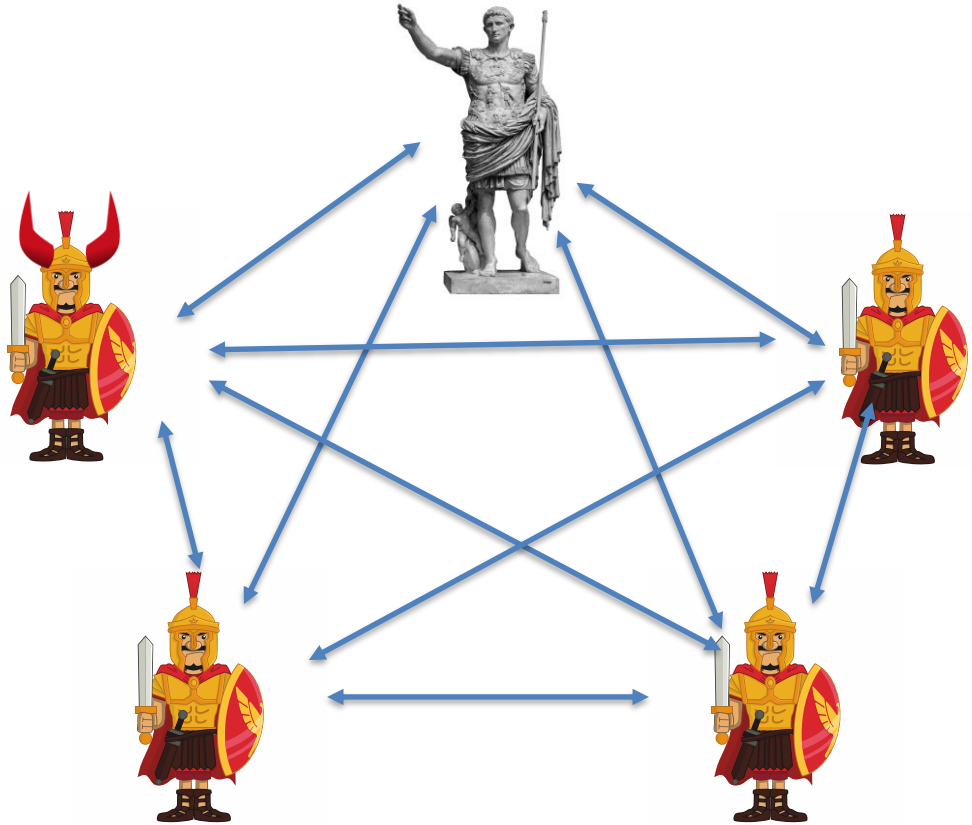
每一轮每个节点可以给其他节点发送消息。消息在下一轮的开始被其他节点收到。

协议结束时每个诚实节点输出一个bit或者退出执行。



拜占庭将军问题

诚实节点遵守协议执行，恶意节点可以做任何操作。



系统有PKI提供认证

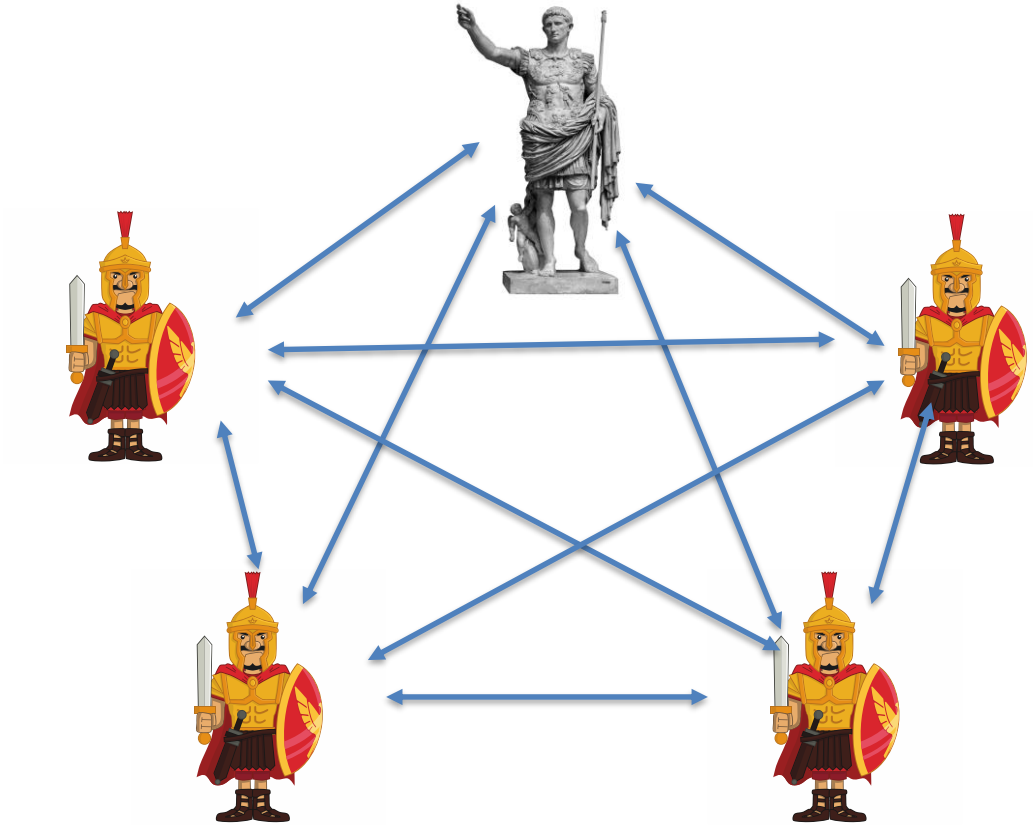
拜占庭将军问题

一致性

如果最终有两个诚实节点输出b和b’，则b=b’。

有效性

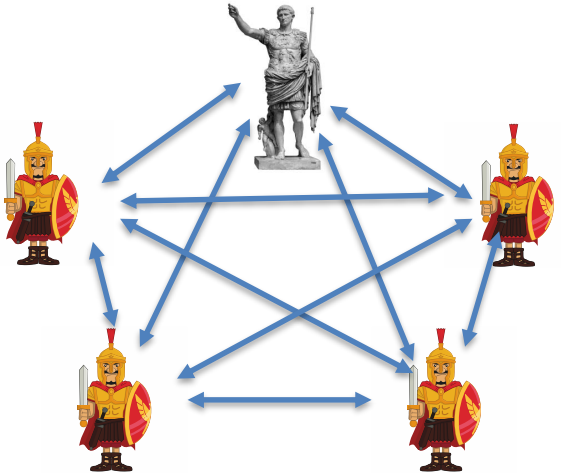
如果首领节点(leader)是诚实的，并且输入b，则所有诚实节点都输出b。



拜占庭将军问题

并不简单

1. 首领节点发送b到所有节点
2. 所有节点转发收到的b到其他节点（投票）
3. 每个节点统计投票结果，输出的票多的结果



如果首领节点是恶意节点？

FLP不可能定理

- Fischer, Lynch and Patterson, 1985， Impossibility of Distributed Consensus with One Faulty Process
  - 在异步通信场景，即使只有一个进程失败，也没有任何算法能保证非失败进程达到一致性

假设	目标
• 异步通信 与同步通信的最大区别是没有时钟、不能时间同步、不能使用超时、不能探测失败、消息可任意延迟、消息可乱序 • 通信健壮 只要进程非失败，消息虽会被无限延迟，但最终会被送达；并且消息仅会被送达一次（无重复） • fail-stop模型与数量 进程失败如同宕机，不再处理任何消息。相对Byzantine模型，不会产生错误消息最多一个进程失败	• Termination（终止性） 非失败进程最终可以做出选择 • Agreement（一致性） 所有的进程必须做出相同的决议 • Validity（合法性） 进程的决议值，必须是其他进程提交的请求值

FLP不可能定理

- 在异步网络中，如果可能存在一个失效停止的节点，则不存在正确的共识协议。
  - 网络状态：同步、异步、半同步
  - 异常节点：失效停止、任意恶意行为
  - 输出结果：确定性共识、概率共识

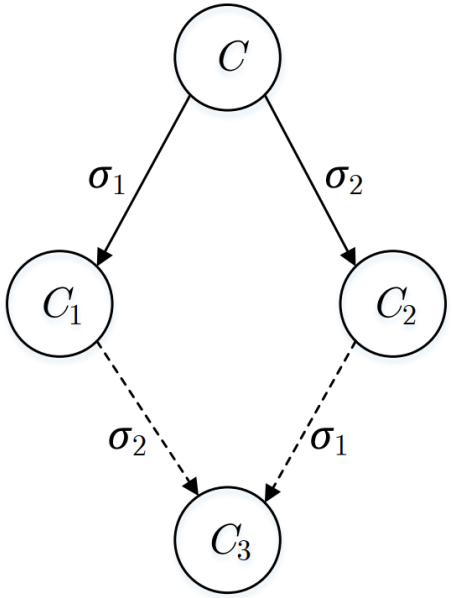
节点执行模型

- 节点p
- 消息缓冲区（p,m)
- Send(p,m)
- Receive(p)
- 任意时刻的全局状态称为一个配置(Configuration), 使用C_i标识不同的配置

规划执行的交换性

- 某个节点受到消息则会改变配置，这个过程称为一个事件$e=(p,m)$，一系列的事件称为一个规划σ

- 引理1
  - 如果两个不同的规划σ_1 σ_2，在规划的执行中参与的节点集合是不相交的，则规划作用在一个相同的初始配置C，其过程是可以交换的。



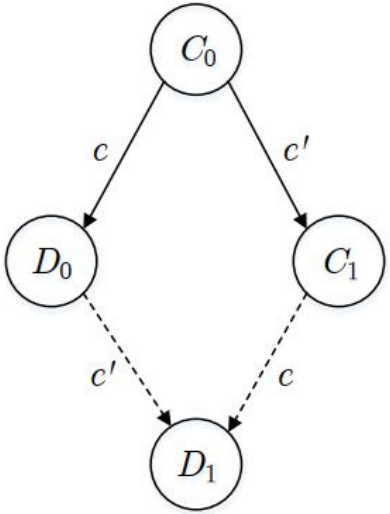
两值配置

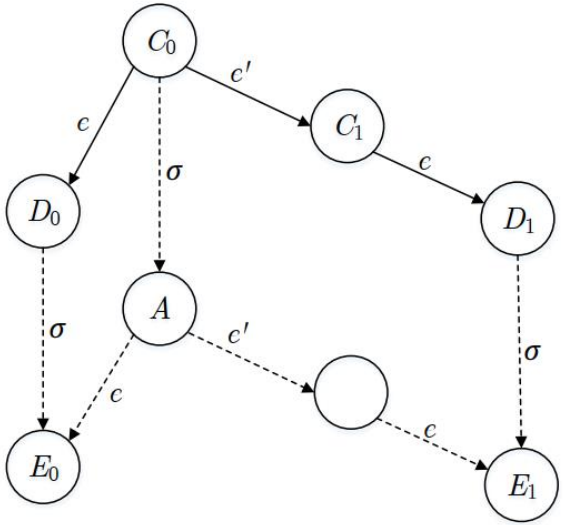
- 如果一个初始配置仅仅输出一个值(0,1)则称为单值配置，否则称为两值配置

- 引理2
  - 在异步网络中，如果存在一个失效停止的节点，则任意正确的共识协议P存在一个两值的初始配置C

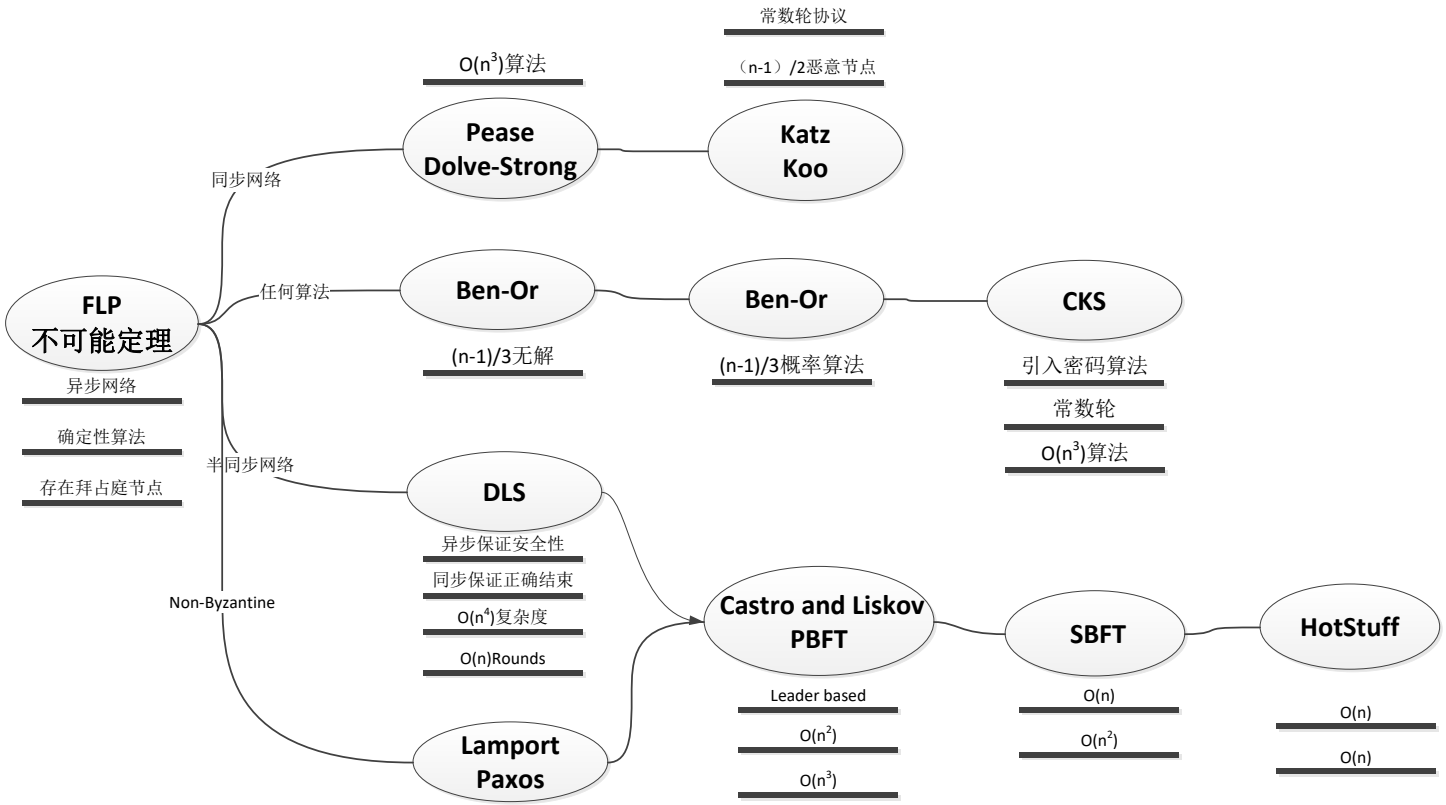
两值配置的持续性

- 引理3
  - 在异步网络中，C是共识协议P的一个两值配置，$e=(p,m)$为可以应用于C的任意一个事件。排除事件e后从C出发所有的可达配置集合E，将e应用于该集合每个元素得到的新集合一定包含两值配置





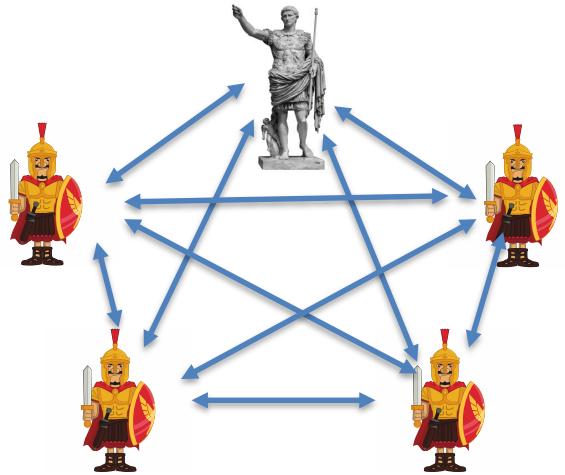
经典共识问题研究路线


FLP
不可能定理
异步网络
确定性算法
存在拜占庭节点
同步网络
Pease
Dolve-Strong
O(n3)算法
Katz
Koo
常数轮协议
（n-1）/2恶意节点
任何算法
Ben-Or
(n-1)/3无解
Ben-Or
(n-1)/3概率算法
CKS
引入密码算法
常数轮
O(n3)算法
半同步网络
DLS
异步保证安全性
同步保证正确结束
O(n4)复杂度
O(n)Rounds
Non-Byzantine
Lamport
Paxos
Castro and Liskov
PBFT
Leader based
O(n2)
O(n3)
SBFT
O(n)
O(n2)
HotStuff
O(n)
O(n)

Dolev Strong 协议

Maximum f corrupt nodes, input message m

1. Leader sends m to all nodes
2. For $r = 1$ to $f + 1$
    1. If you received an unseen message m signed by r signatures (including leader) sign m and send to all. Set $S \leftarrow S \cup \{m\}$
    2. Otherwise remain silent
3. If $|S| = 1$ output $\mathrm{m} \in S$ otherwise output “Confused” (or default message)



f+1 轮
运行效率低

Dolev Strong 例子

f=2

Brutus

Marc Anthony

Pompeius

Augustus

Dolev Strong 例子

f=2
r=1

Attack=1

Brutus

$1_{Caesar,MA}$

Marc Anthony

Pompeius

$1_{Caesar, Aug}$

Augustus

Dolev Strong 例子

f=2
r=2

Attack=1

Brutus

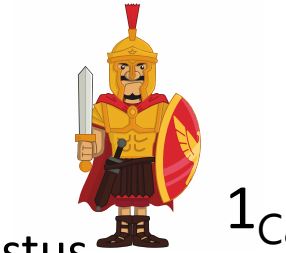
REJECTED

Marc Anthony

$1_{Caesar,MA}$

$0_{Brutus,Pompeius}$

Pompeius



Augustus

$1_{Caesar, Aug}$

Dolev Strong 例子

f=2
r=3

Attack=1

Brutus

Marc Anthony

1Caesar, Aug, MA

Pompeius

Augustus

1Caesar, MA, Aug

Dolev Strong 例子

f=2
r=3

Attack=1

Brutus

1 Caesar,MA

Marc Anthony

Pompeius

1 Caesar, Aug

Augustus

Dolev Strong 例子

f=2
r=3

Attack=1

Attack

1 Caesar,Aug,MA

Marc Anthony

Brutus

Pompeius

Attack

1 Caesar, MA, Aug

Augustus

超过f个恶意节点

f=2
r=3

Brutus

1 Caesar,MA

Marc Anthony

0 Caesar,Brutus,Pompeius

Pompeius

1 Caesar, Aug

Augustus

超过f个恶意节点

f=2
r=3

Brutus

Pompeius

Confused

0 Caesar,Brutus,Pompeius

1 Caesar,Aug,MA

Marc Anthony

Attack

1 Caesar, Aug, MA

Augustus

Dolev Strong 协议分析

为什么需要 f+1 轮?

f 个恶意节点可以生成f个有效签名

Validity?

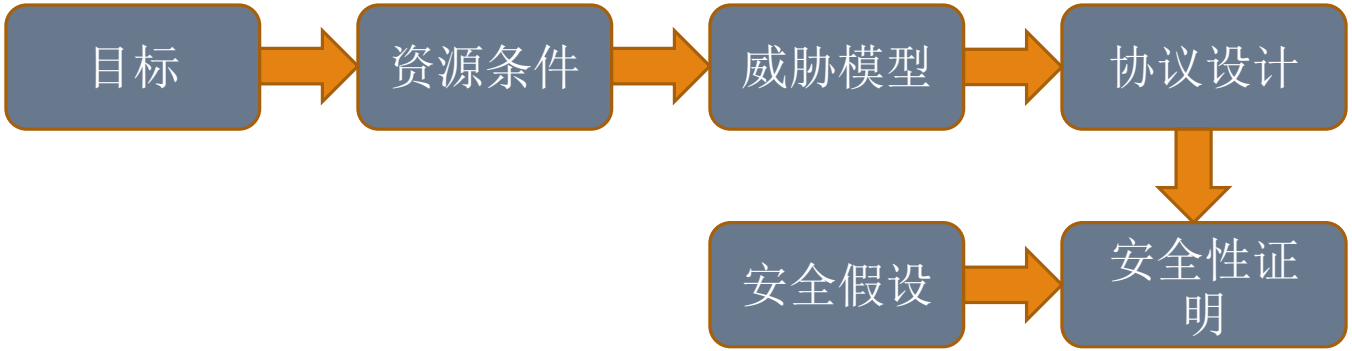
诚实节点只接受包含leader发出的有效签名的消息

Consistency?

1. If honest node has $\mathrm{m} \in S$ at round $r \leq f$ then all other nodes will have $\mathrm{m} \in S$ at $r+1$
2. If honest node receives new m at round $f+1$ then it must have received it from an honest node
3. -> All honest nodes have identical S

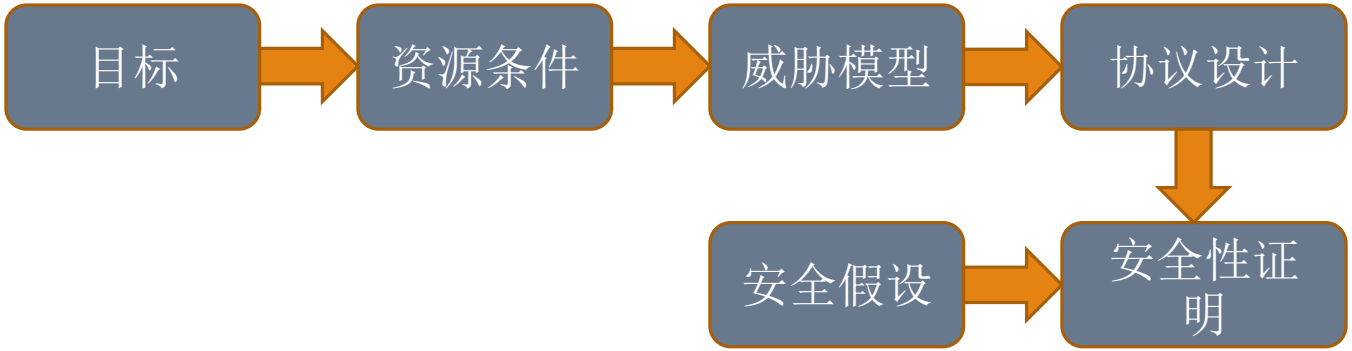
密码协议设计分析模型

密码协议分析的一般模型

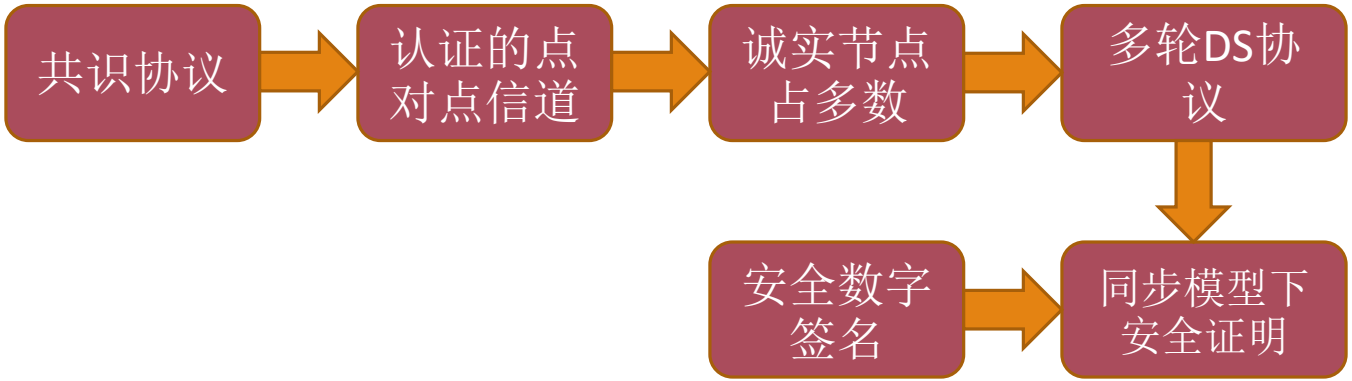


经典共识协议设计分析模型

密码协议分析的一般模型

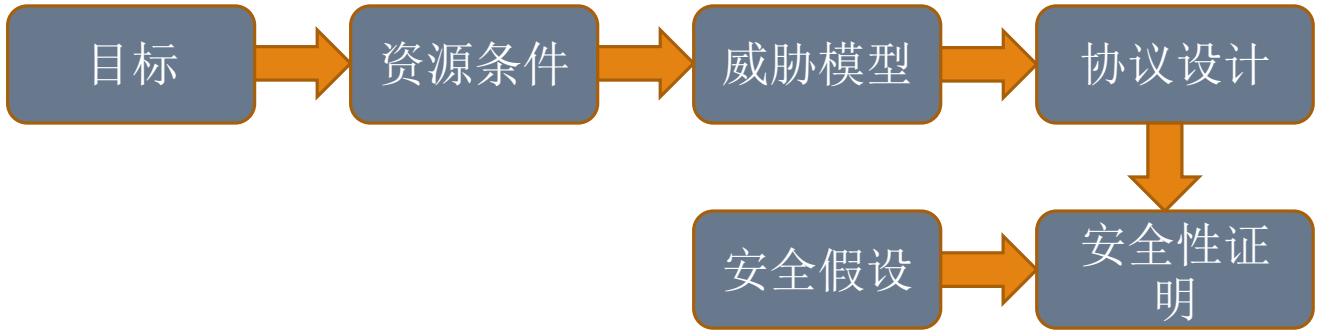


Dolev-Strong协议分析模型

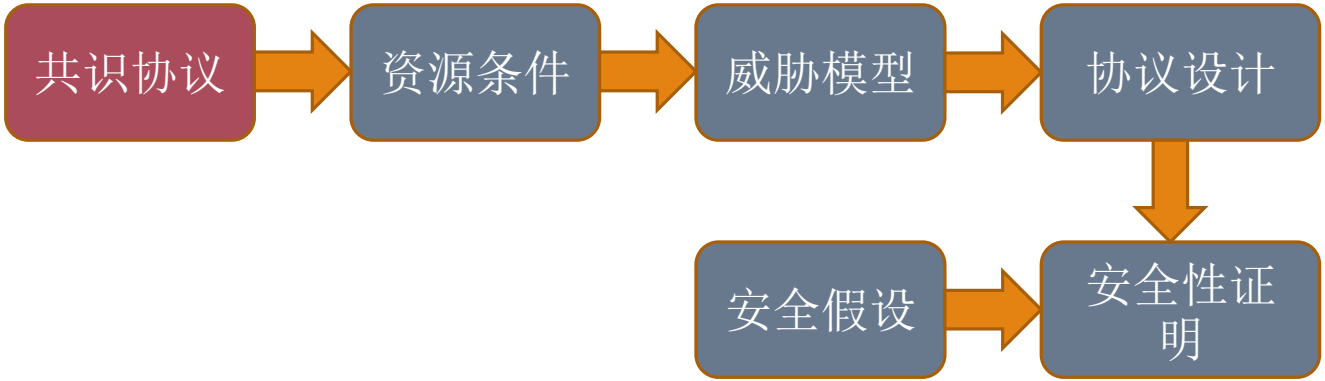


PoW区块链分析模型

密码协议分析的一般模型

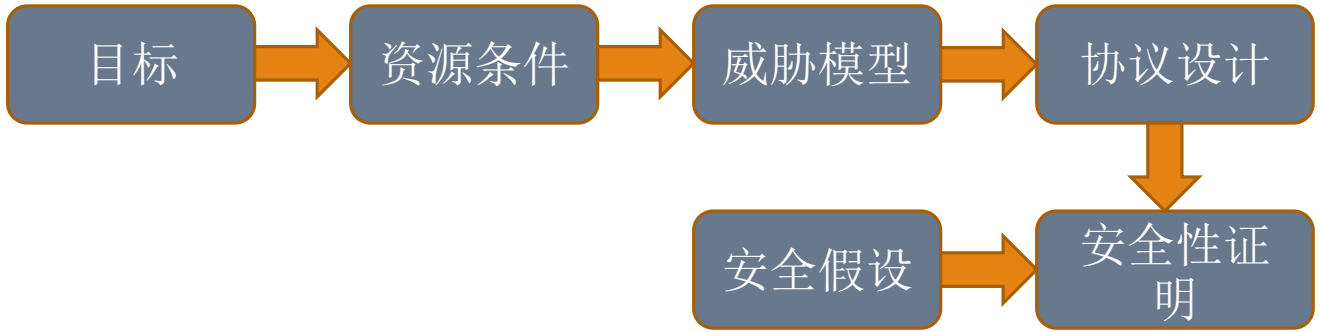


PoW区块链协议分析模型

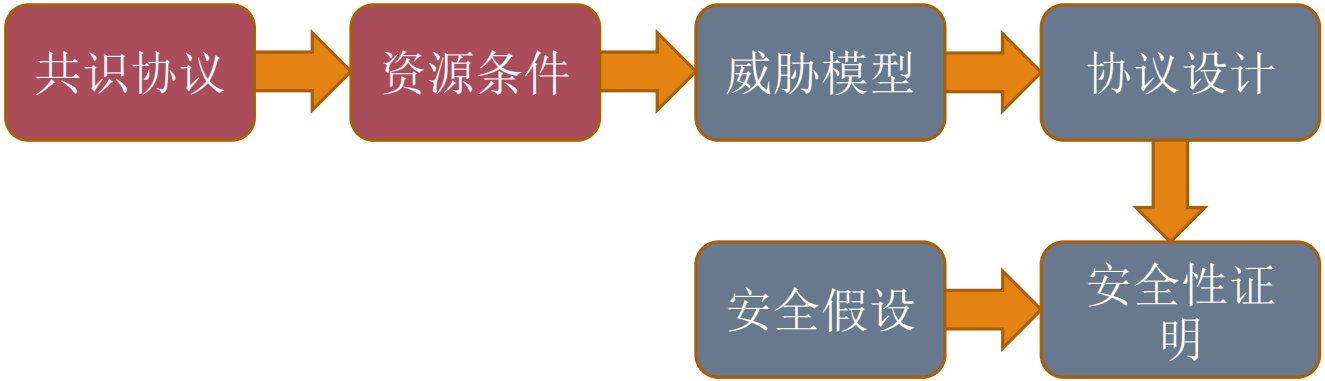


PoW区块链分析模型

密码协议分析的一般模型

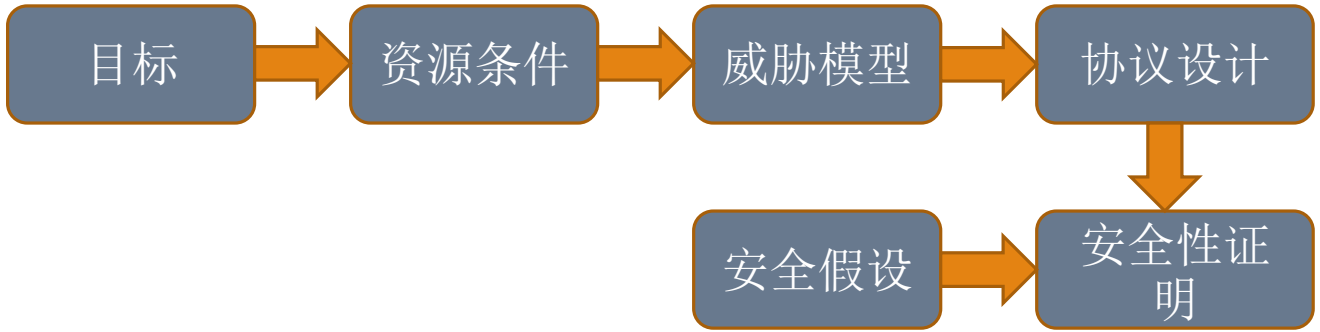


PoW区块链协议分析模型

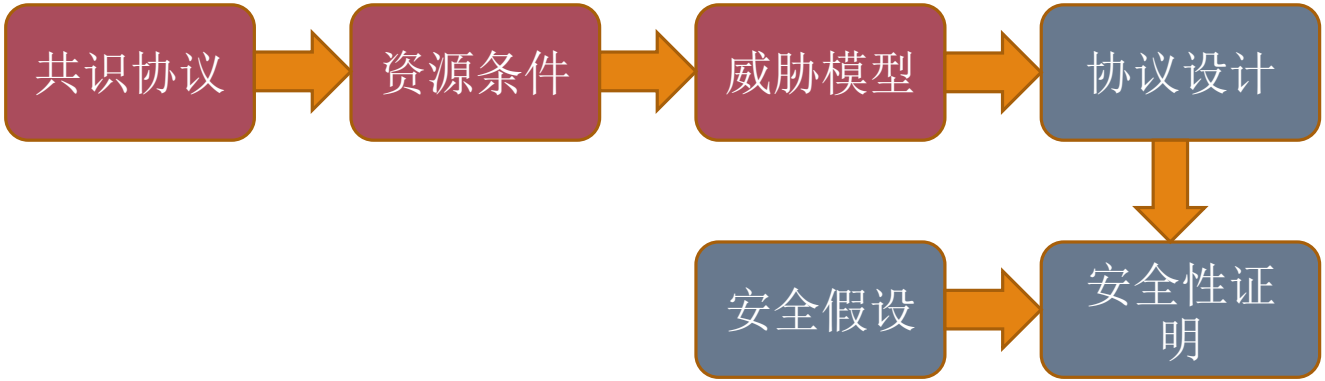


PoW区块链分析模型

密码协议分析的一般模型

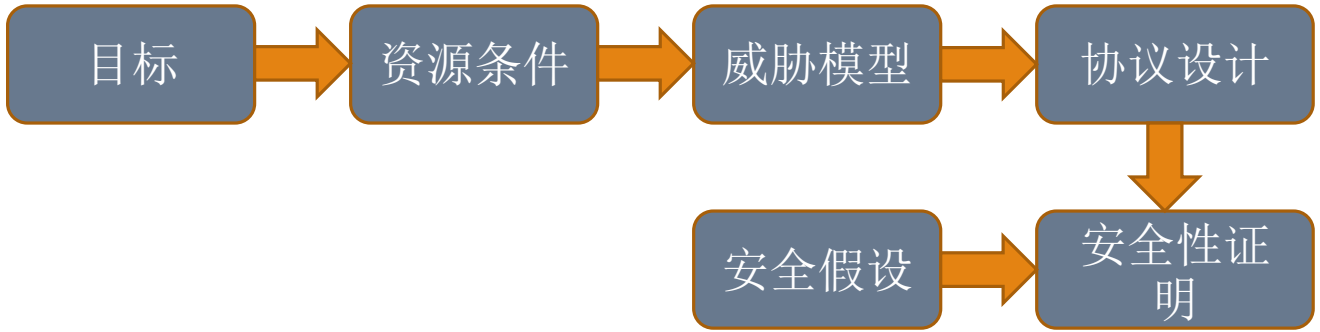


PoW区块链协议分析模型

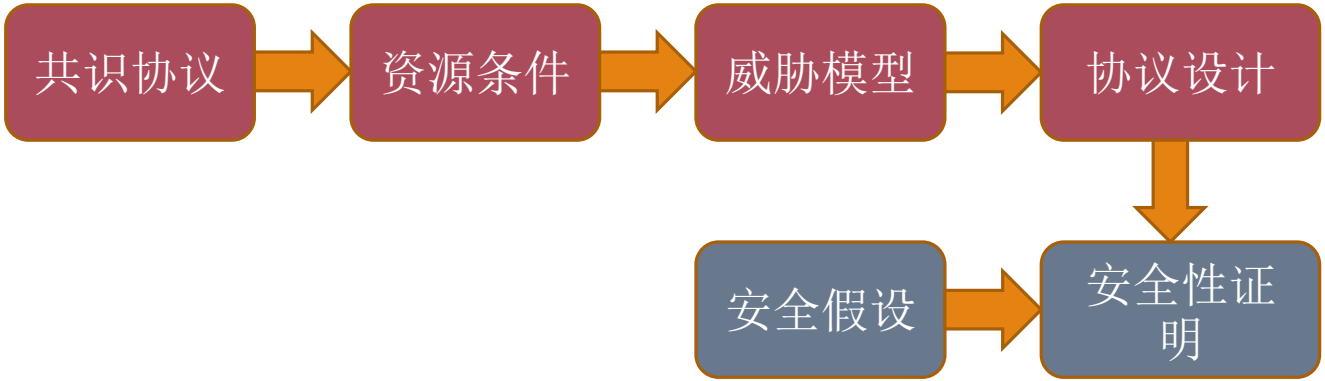


PoW区块链分析模型

密码协议分析的一般模型

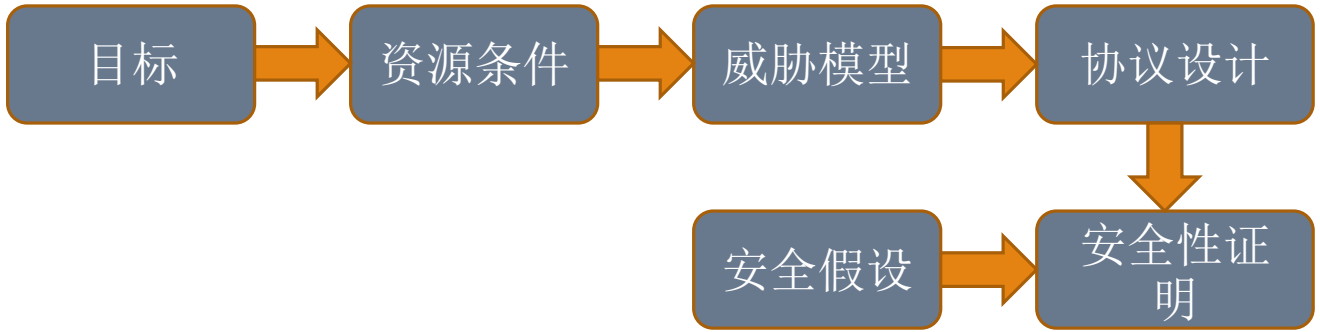


PoW区块链协议分析模型

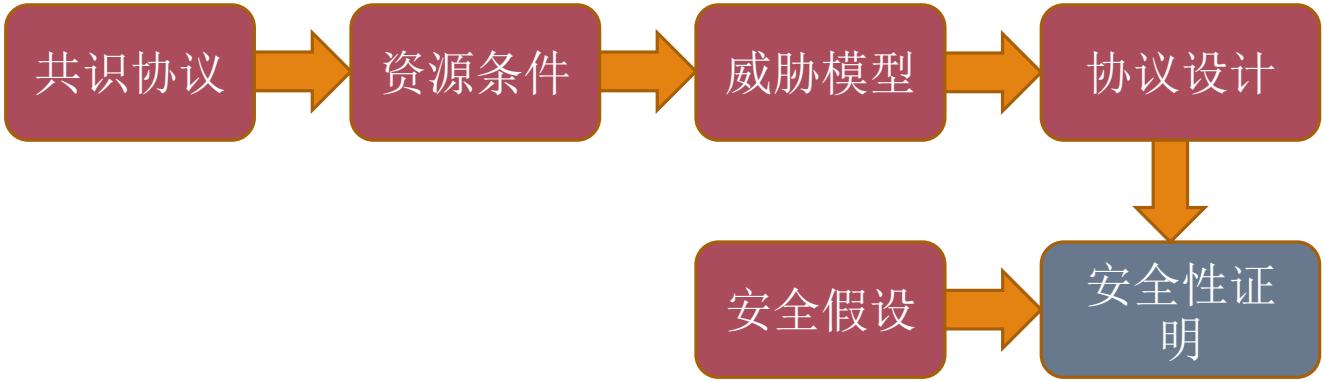


PoW区块链分析模型

密码协议分析的一般模型

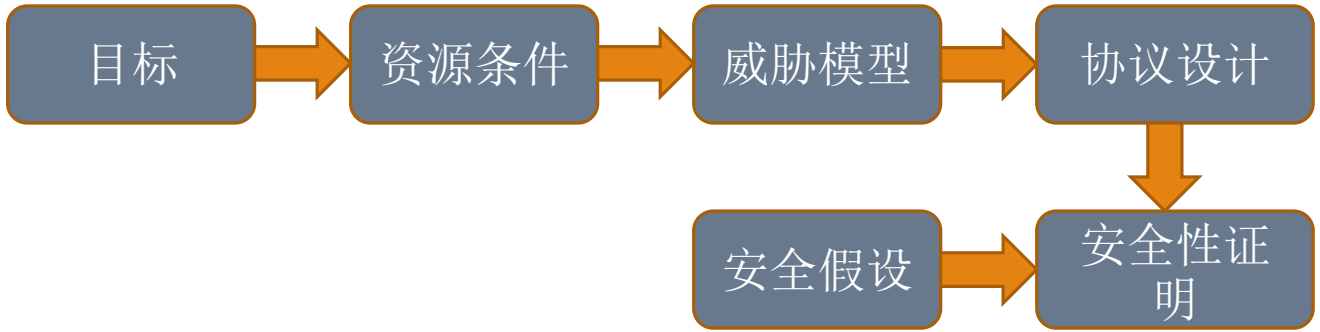


PoW区块链协议分析模型

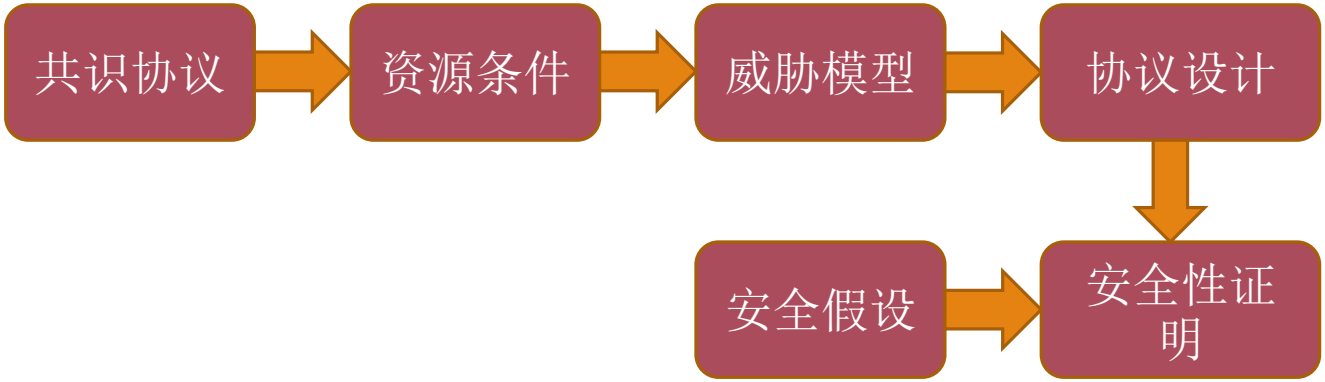


PoW区块链分析模型

密码协议分析的一般模型



PoW区块链协议分析模型



谢谢