区块链其他

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

上次课程内容

1 浏览器指纹

- Web跟踪
- 简介
- 技术
- 防范

2 物理安全

- 物理防护
- 安全打印
- 物理攻击
- 中继攻击

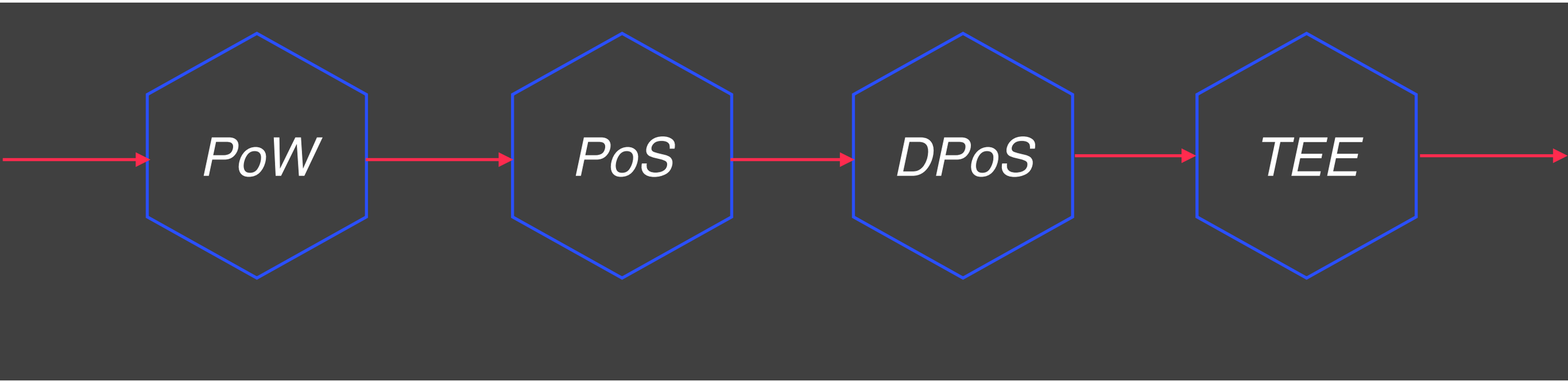
3 访问控制

- 定义
- 模型
- 行为
- 策略

4 身份管理

- 身份
- 身份管理
- 分类
- 服务/链

共识算法



共识模型

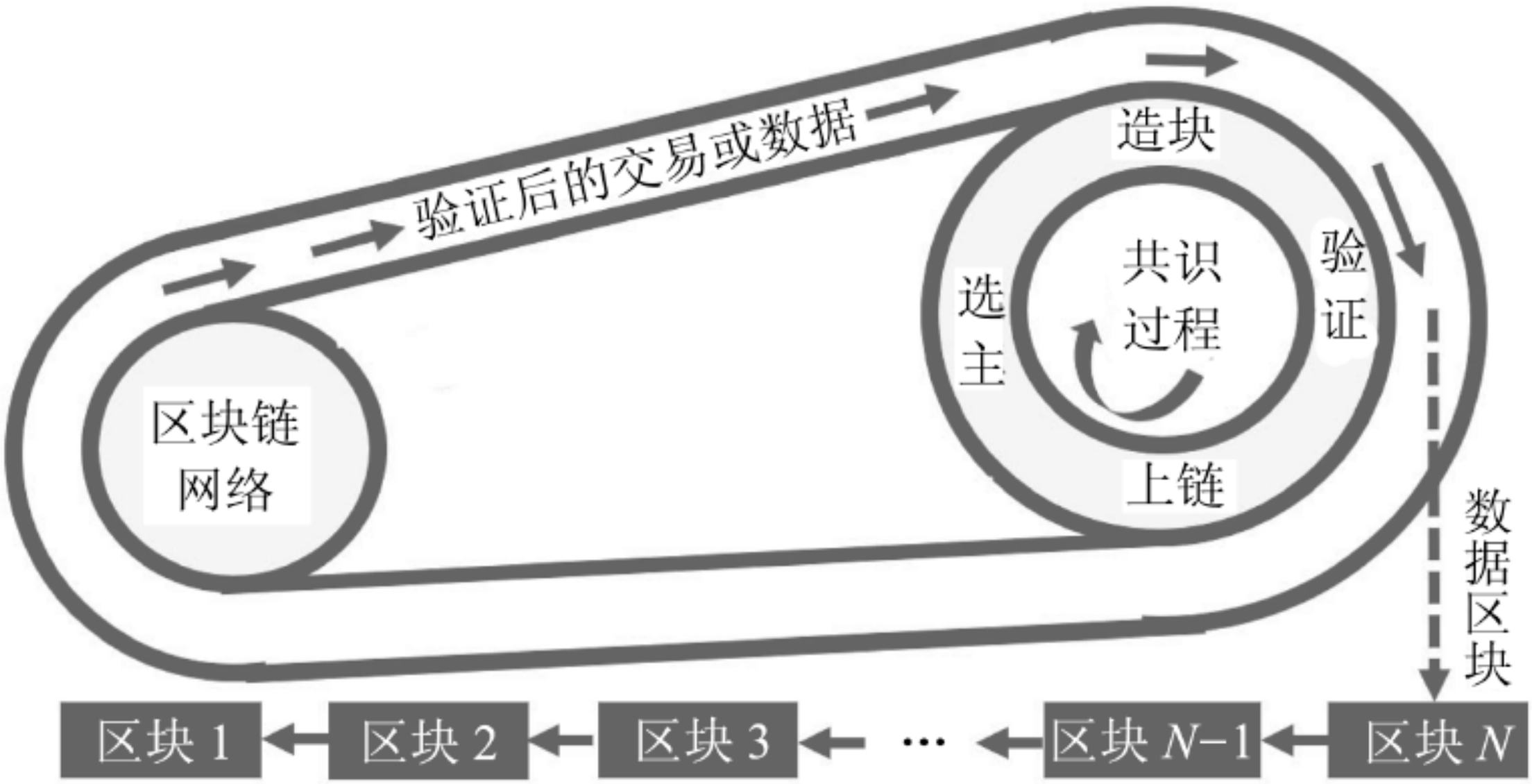


图 1　区块链共识过程的基础模型

共识算法

目的：在特定的**网络模型和故障模型**前提下, 如何在缺乏中央控制和协调的分布式网络中确保**一致性**。（群龙无首）

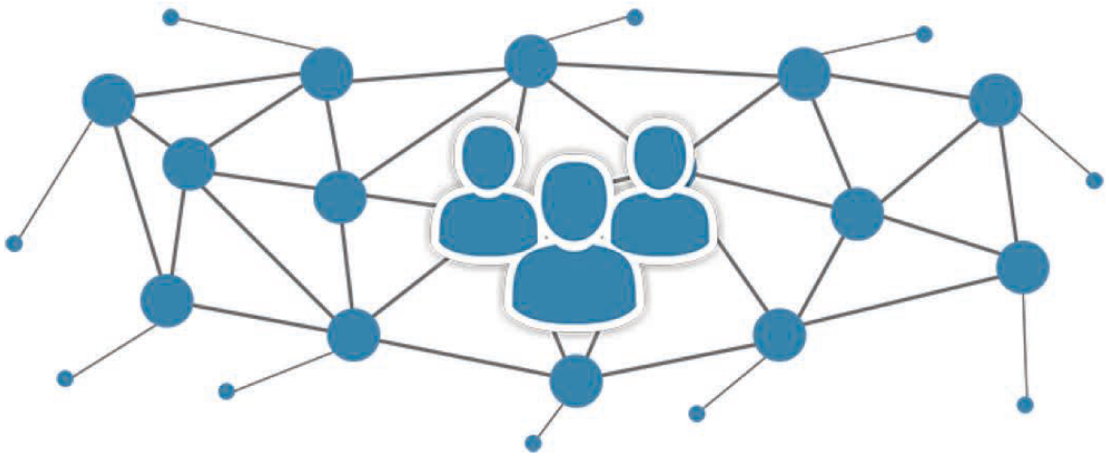
基础理论：拜占庭将军问题

过程：选举 、出块、验证 、上链

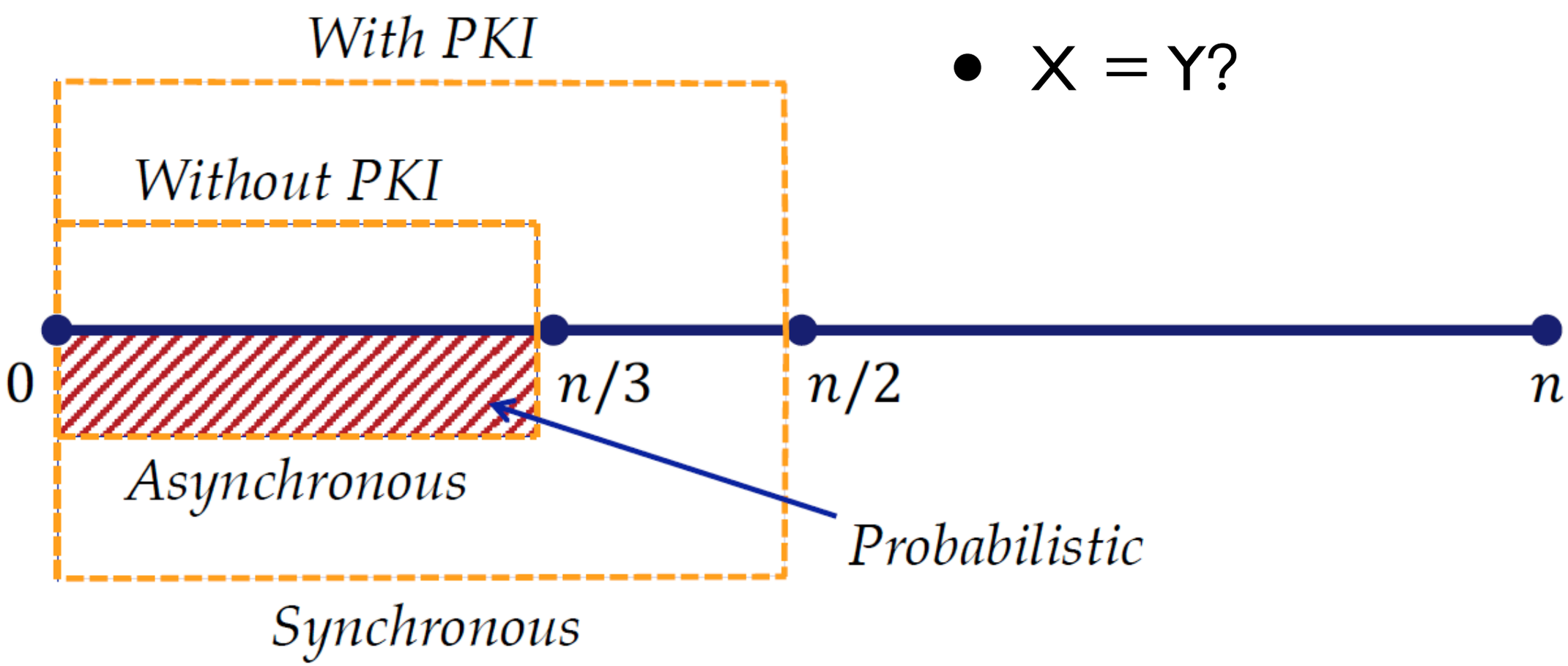
根据选举策略分类：选举类（Paxos）、证明类（pow）、随机类（PoET）、联盟类（DPoS）和混合类（pow+pos）

根据演进方向分类：pow,pos,pow+pos,传统分布式一致性算法的改进及其他有明显的创新之处, 具有一定的大规模应用的前景。

传统的共识



- N个节点，T个拜占庭节点
- 广播X
- 所有诚实节点输出Y
- X = Y?



PoW类

Pow类基本思想：矿工节点在每一轮共识过程中必须证明自己具有 某种特定的能力, 证明方式通常是竞争性地完成某 项难以解决但易于验证的任务, 在竞争中胜出的矿工节点将获得记账权

改进方向：扩容或者降低能耗以提高效率和公平。

典型代表:

- Proof Of Work（pow）
- Proof Of Elapsed Time（poet）
- Proof Of Luck(pol)
- Proof Of Useful Work（pouw）

PoUW

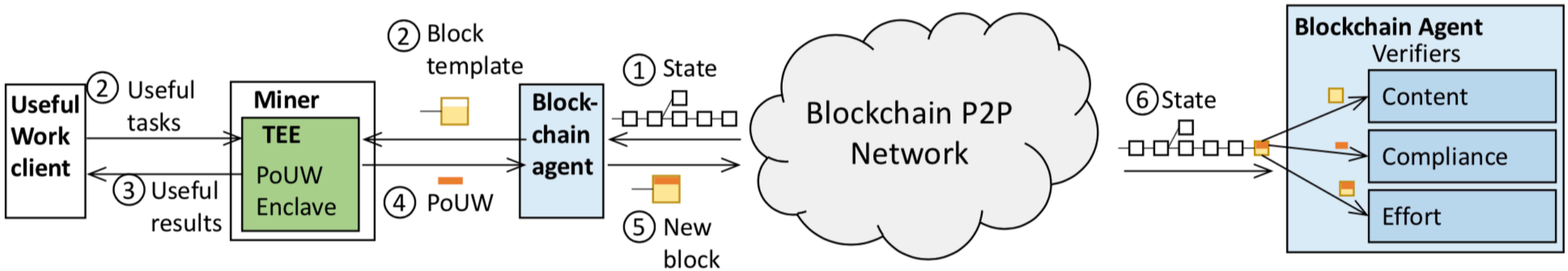
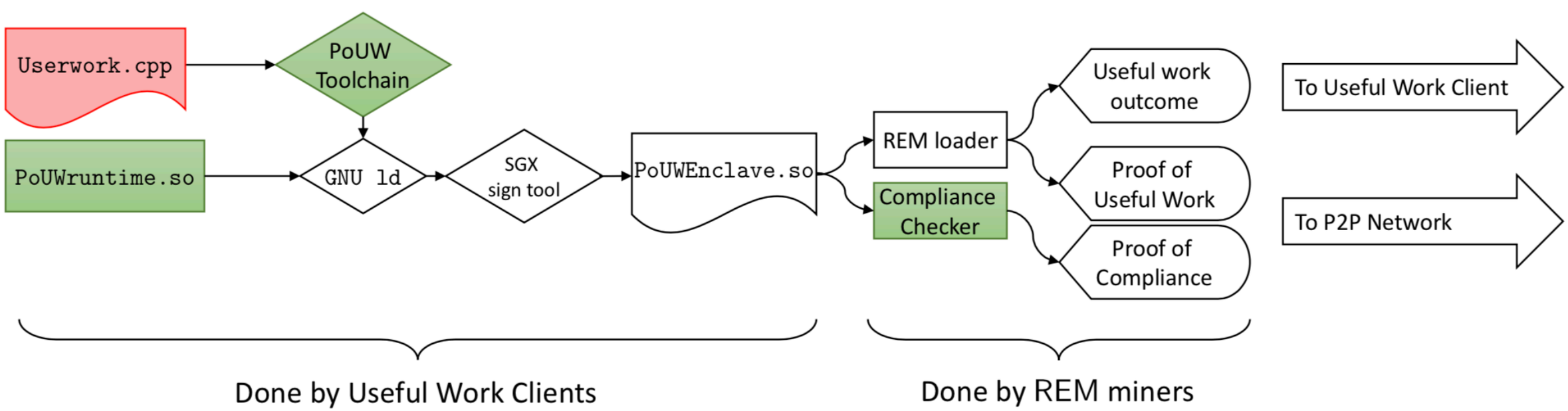


Figure 1: Architecture overview of REM



PoS

每个领导者被选出的概率与持有股份数量成比例，被选出的领导者可以生成区块。

—Janno Siim：Proof-of-Stake Research Seminar in Cryptography

POW

- 全体节点
- 无抵押
- 耗费资源

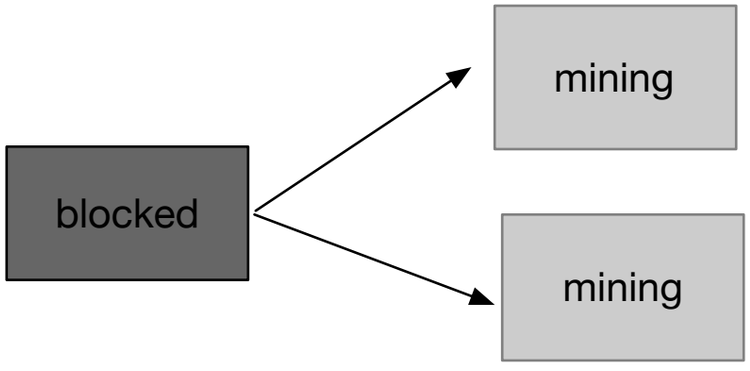
POS

- 验证人工作组
- 财产抵押
- 少量计算资源

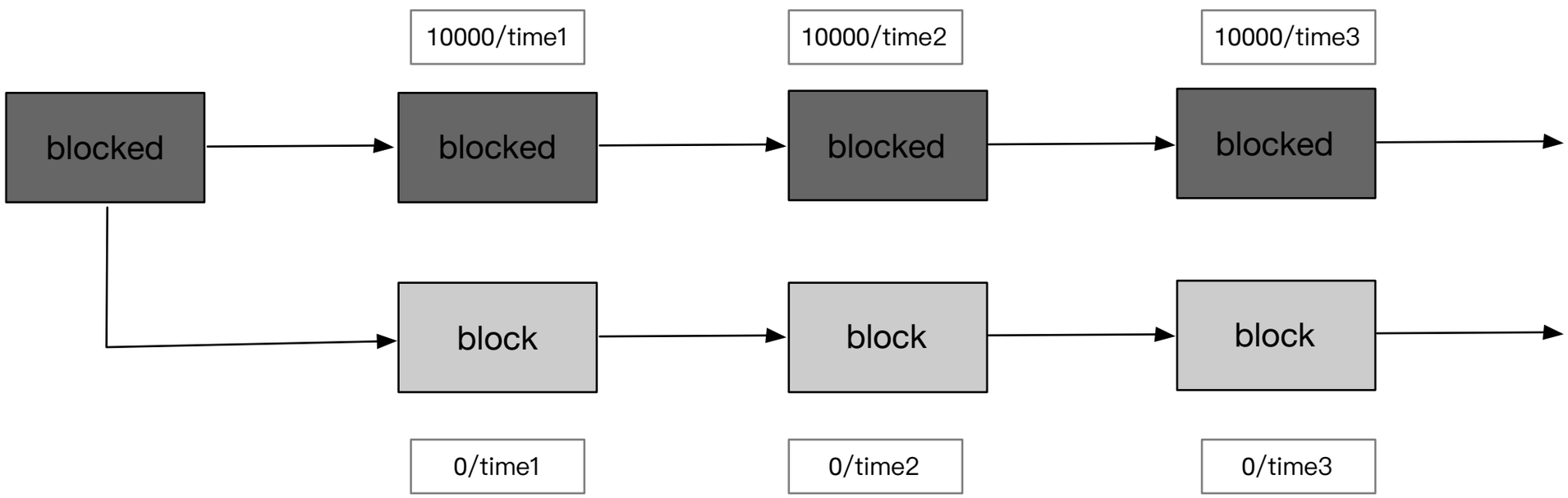
hash=<target

hash=<target * coinage

PoS攻击



- POS挖矿资源消耗的低
- 矿工在分叉链上挖矿消耗少
- 矿工可以同时挖分叉链
- 没有相应的限制和惩罚
- Deposit-based PoS



TEE + PoS

TEE： Trusted Execution Environments

1）独立于操作系统的一个执行区

2）提供一些密码函数和限制操作系统内存读写

3） **montonic counter 单调计数器**

TEE-based Pos

1) 资格证明和块签名由TEE产生。

2）用单调计数器保障每个高度最多产生一个快

3）两个单调计数器CTRep和CTRbs

4) CTRep记录已经提交的资格签名的块高度，CTRep记录已经提交的区块签名的块高度

5) 块高度H的出块资格条件 CTRep<H

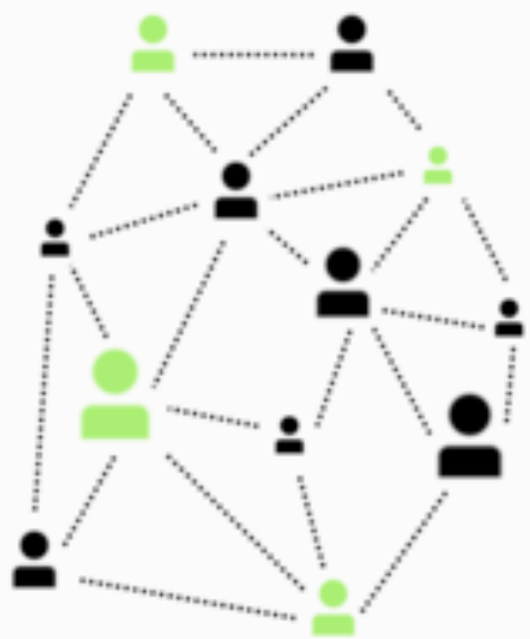
6）验证器签名块的条件 CTRbs<H

DPoS

Electing witnesses in a Delegated Proof-of-Stake network

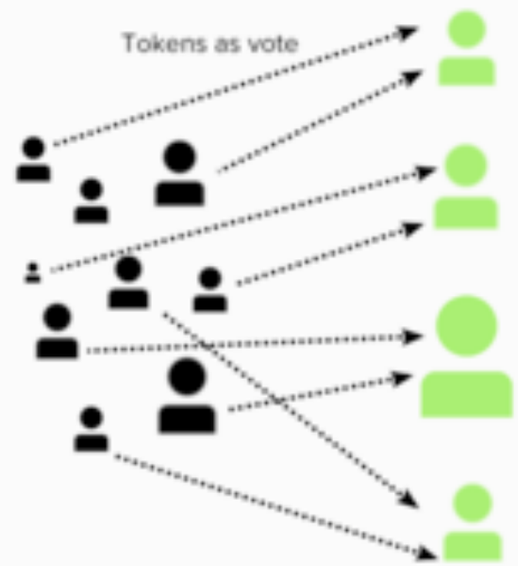
nichanank.com

1.



Nodes express interest in becoming a witness and begin lobbying, making positive contributions to the network and engaging the community.

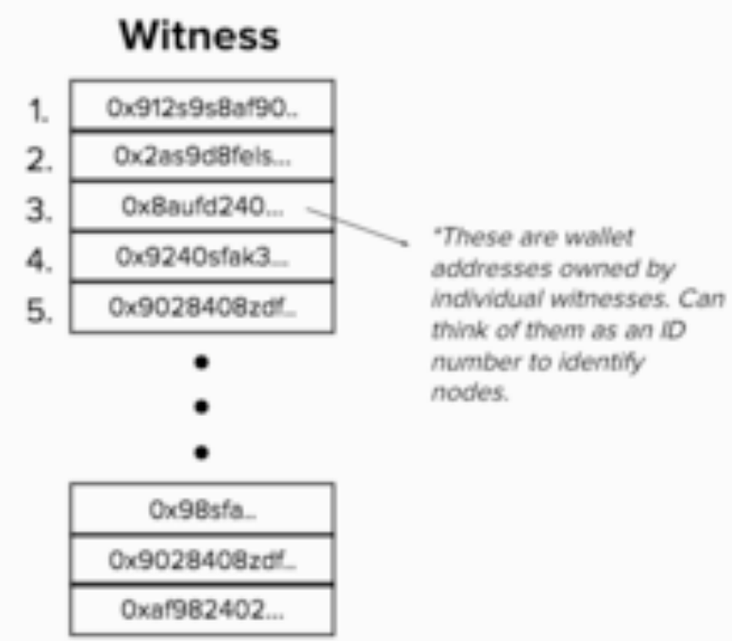
2.



People in the network allocate their tokens as **votes** for witnesses

The more tokens they have, the higher their voting weight - hence *proof of stake**

3.



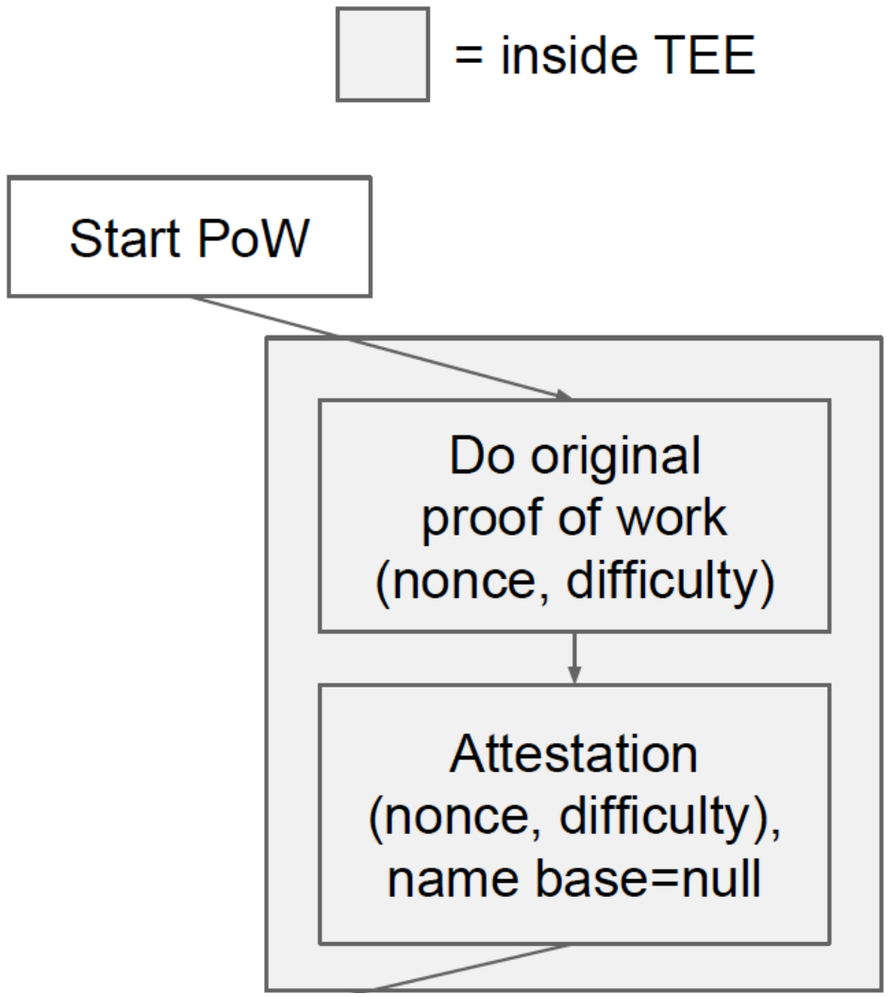
We end up with a ranking of nodes with the most votes (# tokens allocated to them).

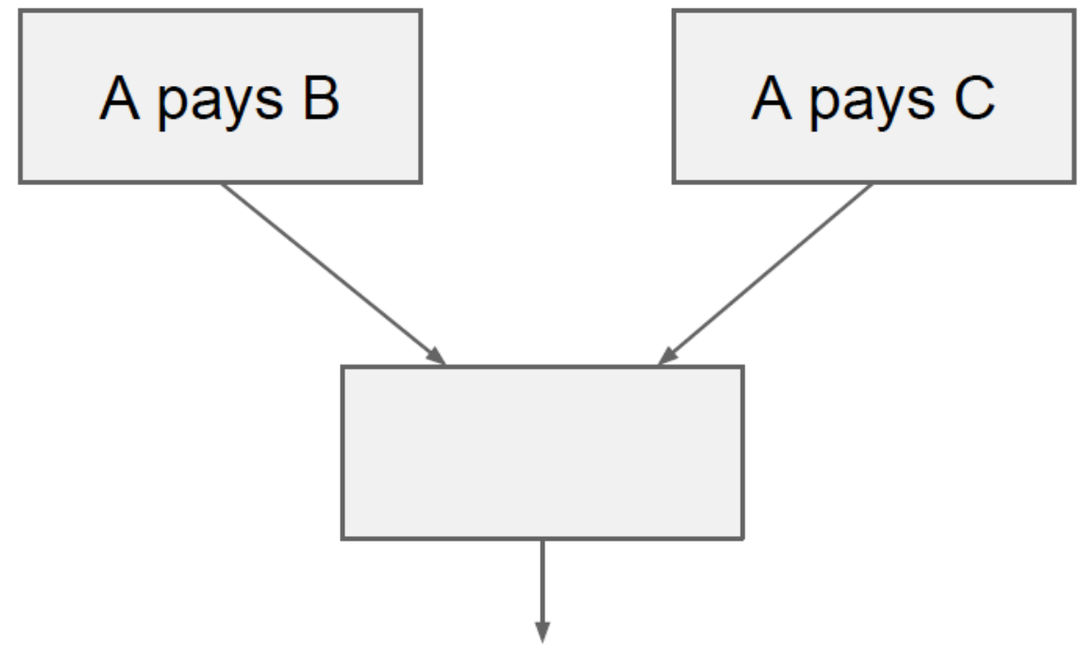
The top N of these will become members of the elected witness panel. N depends on the network.

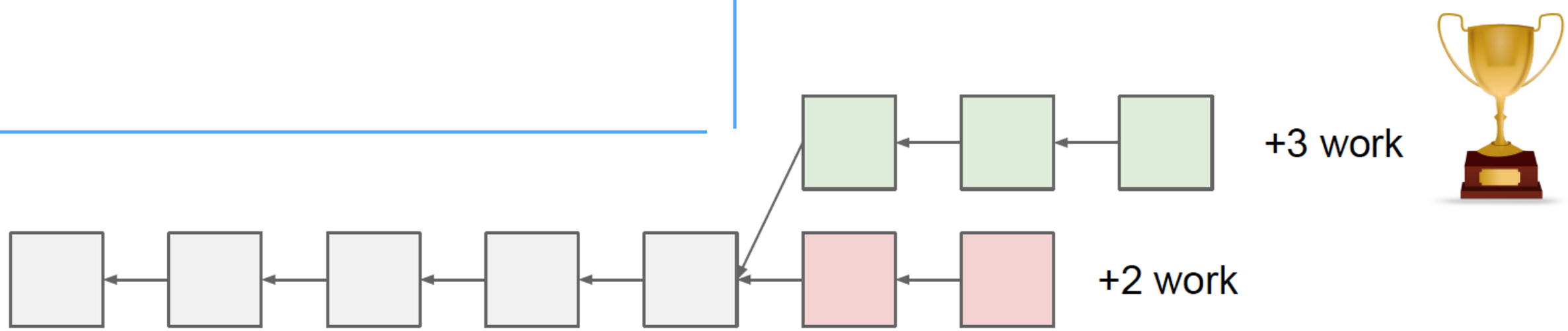
*Participants are NOT *giving* tokens to their witnesses. They are merely *alloting* funds to their choices as an expression of their vote. They can reassign their tokens to another witness at any time.

EOS

共识 + TEE

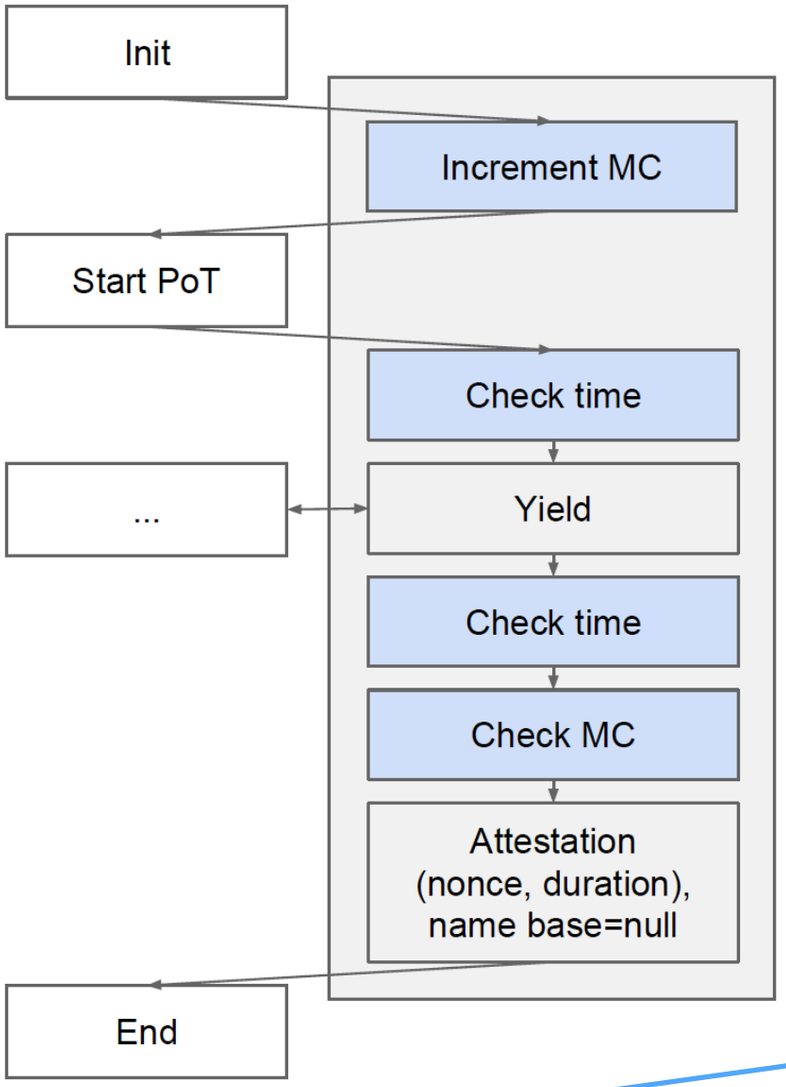

= inside TEE
Start PoW
Do original proof of work (nonce, difficulty)
Attestation (nonce, difficulty), name base=null

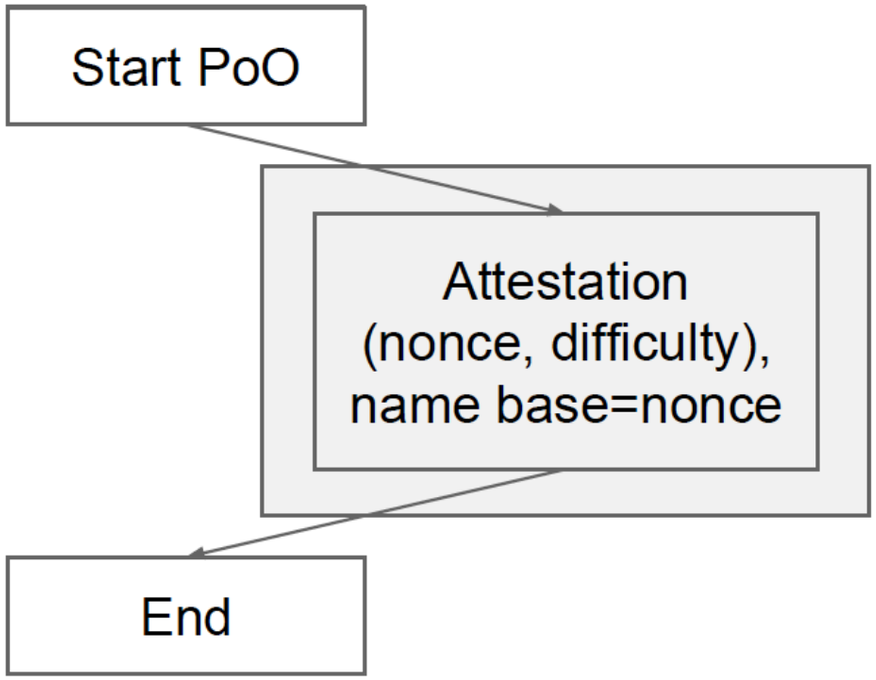

A pays B
A pays C


+3 work
+2 work

Consensus

共识 + TEE

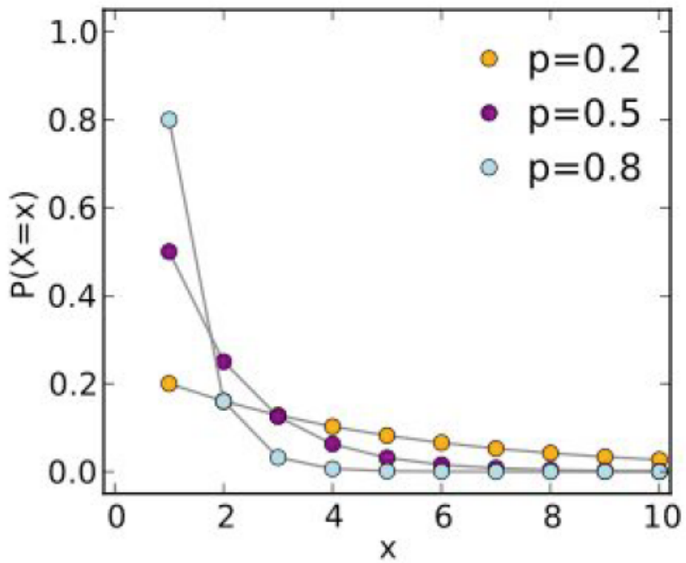




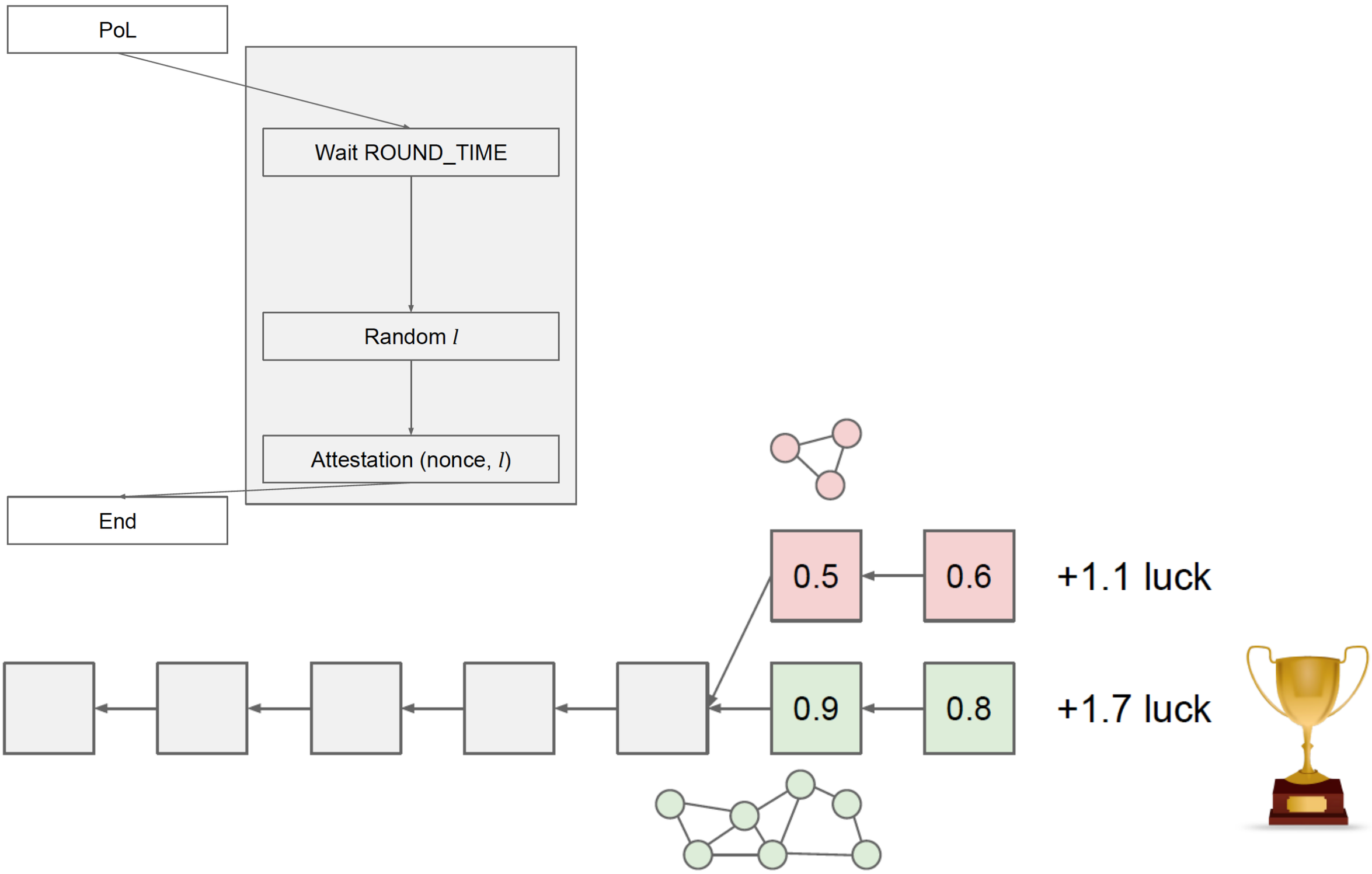

```
598fc24b...
c052d575...
d824325d...
fd3f6615...
f2c4d943...
d9799954...
fb2eb5e0...
439696f5...
c7882894...
00000000...
```

X ~ geometric distribution

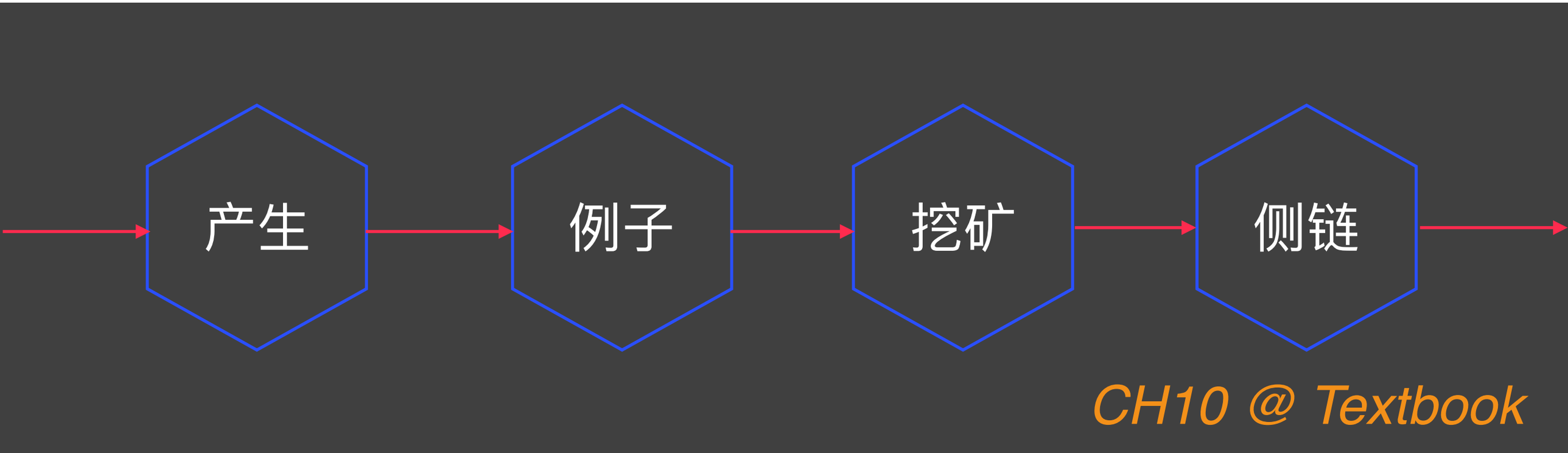
$$\Pr[X=x]=(1-p)^{k-1}p$$



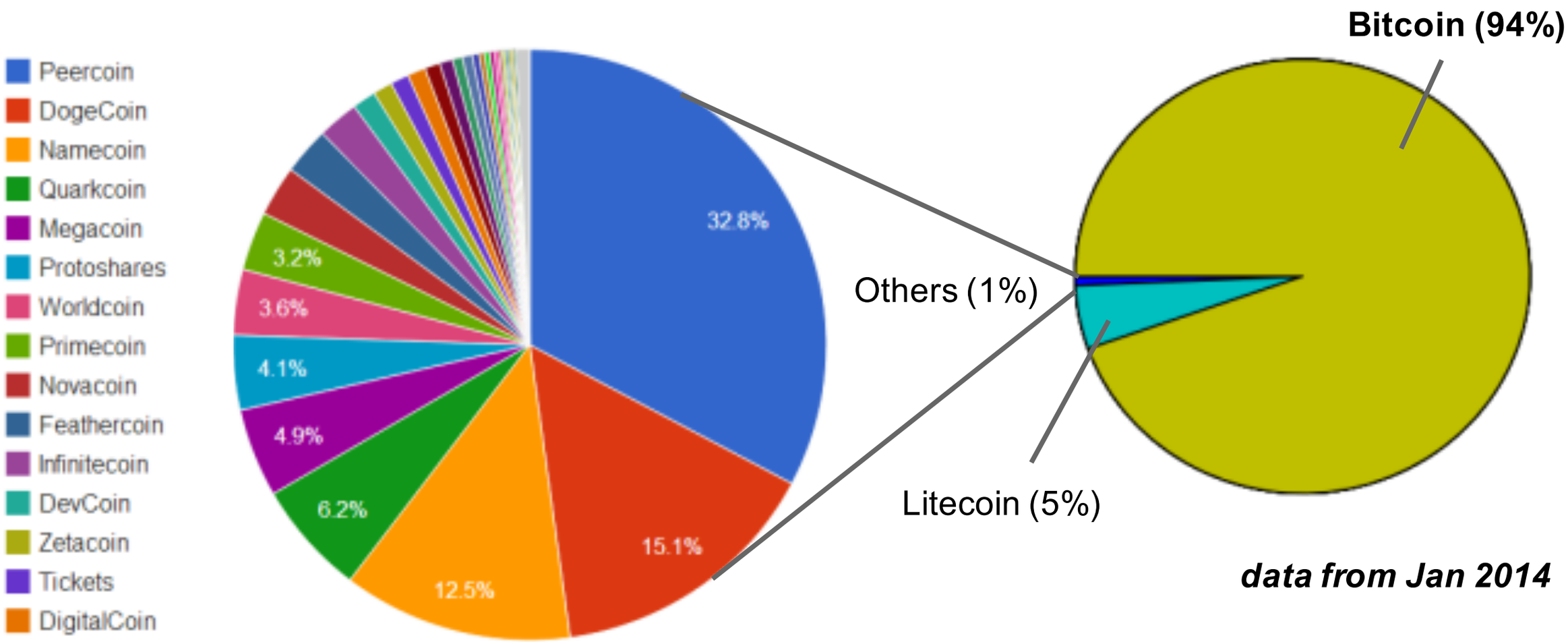
PoL


PoL
Wait ROUND_TIME
Random l
Attestation (nonce, l)
End
0.5
0.6
+1.1 luck
0.9
0.8
+1.7 luck

另类币



加密货币



data from Jan 2014

一些代币

为什么发行

吸引矿工

如何发行

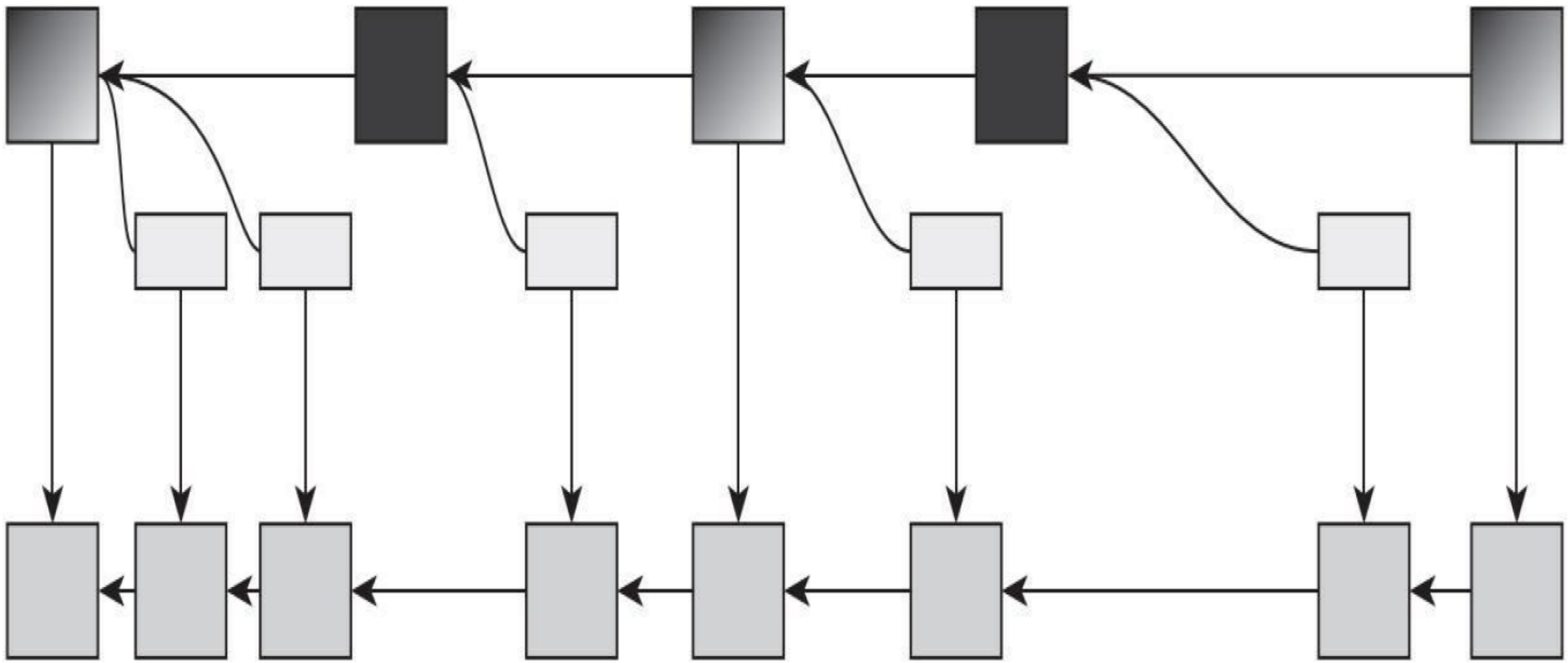
拉高出货

初始分配

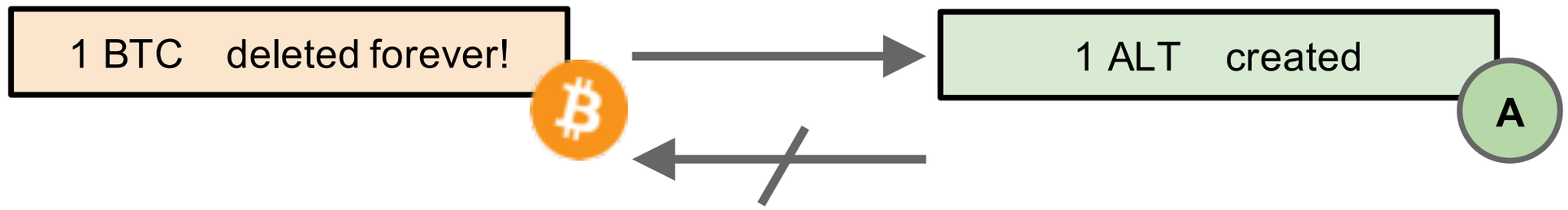
挖矿攻击

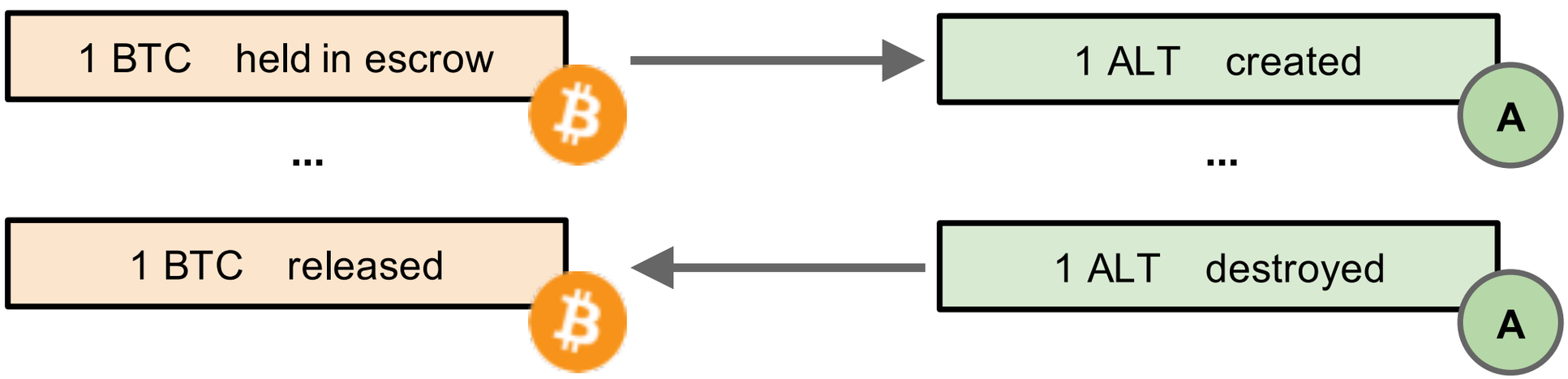
共同挖矿

共同挖矿



侧链


1 BTC deleted forever!
1 ALT created
A


1 BTC held in escrow
1 ALT created
A
...
...
1 BTC released
1 ALT destroyed
A

00001010
00000010
00001110
00000110

更多的链正在路上

ethereum

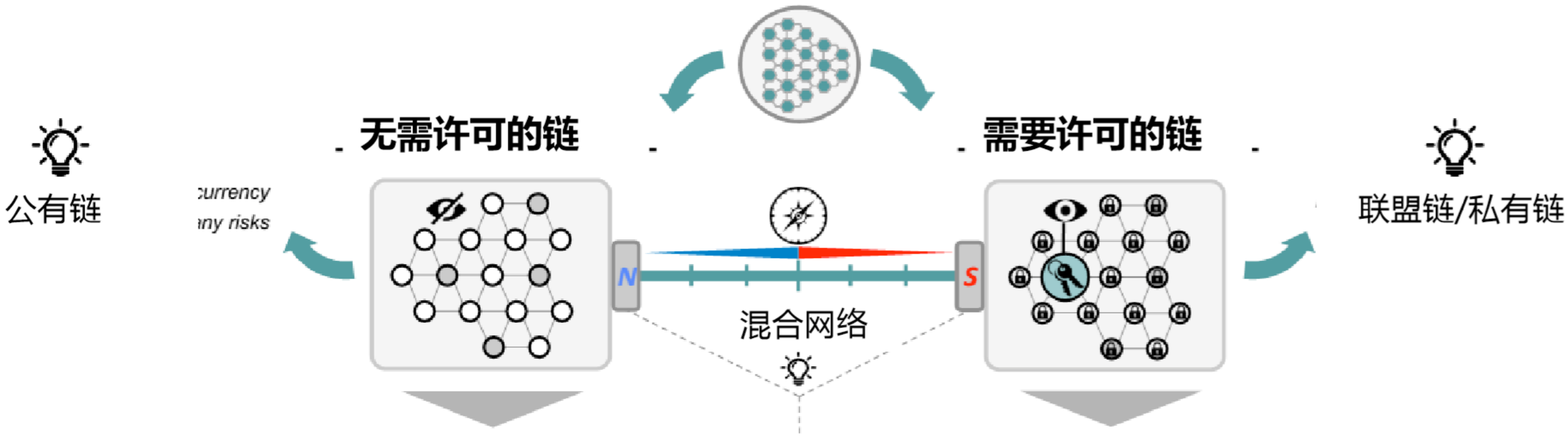
金色财经jinse.com
IPFS
IPFS is The Permanent Web
A new peer-to-peer hypermedia protocol

EOS
Decentralize Everything
比特智投

HYPERLEDGER

超级账本

联盟链



• 用户匿名	• 用户验证
• 网络接入不受限	• 网络接入需要管控
• 账本写入的见证者列表是不确定的	• 账本写入的见证者列表是确定的
• 没有系统管理员	• 有系统管理员，可配置和管控系统

共识算法

大概率一致的共识算法

绝对一致的共识算法

特性	POW	POS	DPOS	PBFT	RBFT
节点管理	公开	公开	公开	准入机制	准入机制
交易延时	高（分钟）	低（秒级）	低（秒级）	低（毫秒级）	低（毫秒级）
吞吐量	低	高	高	高	高
节能	否	是	是	是	是
安全性	<=51%算力	<=49%股权	<=49%验证	<=33.3%恶意节点	<=33.3%恶意节点
代表应用	bitcoin、ethereum	peercoin	Bitshare	Fabirc	Hyperchain
扩展性	好	好	好	差	差

一般用于非许可（公有）链

一般用于许可（联盟）链

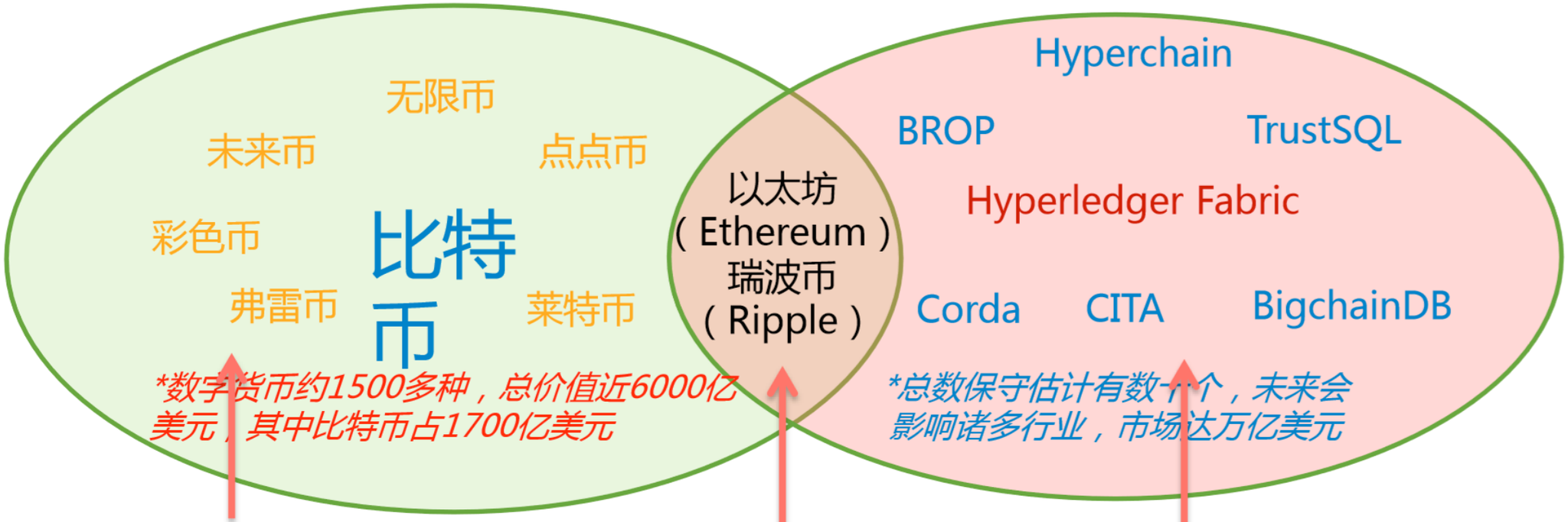
币和链

币圈

在区块链上发行加密数字货币，进行价值交换

链圈

用区块链技术解决企业信息化问题，传递信任



公有链用币做激励

有重合的地方

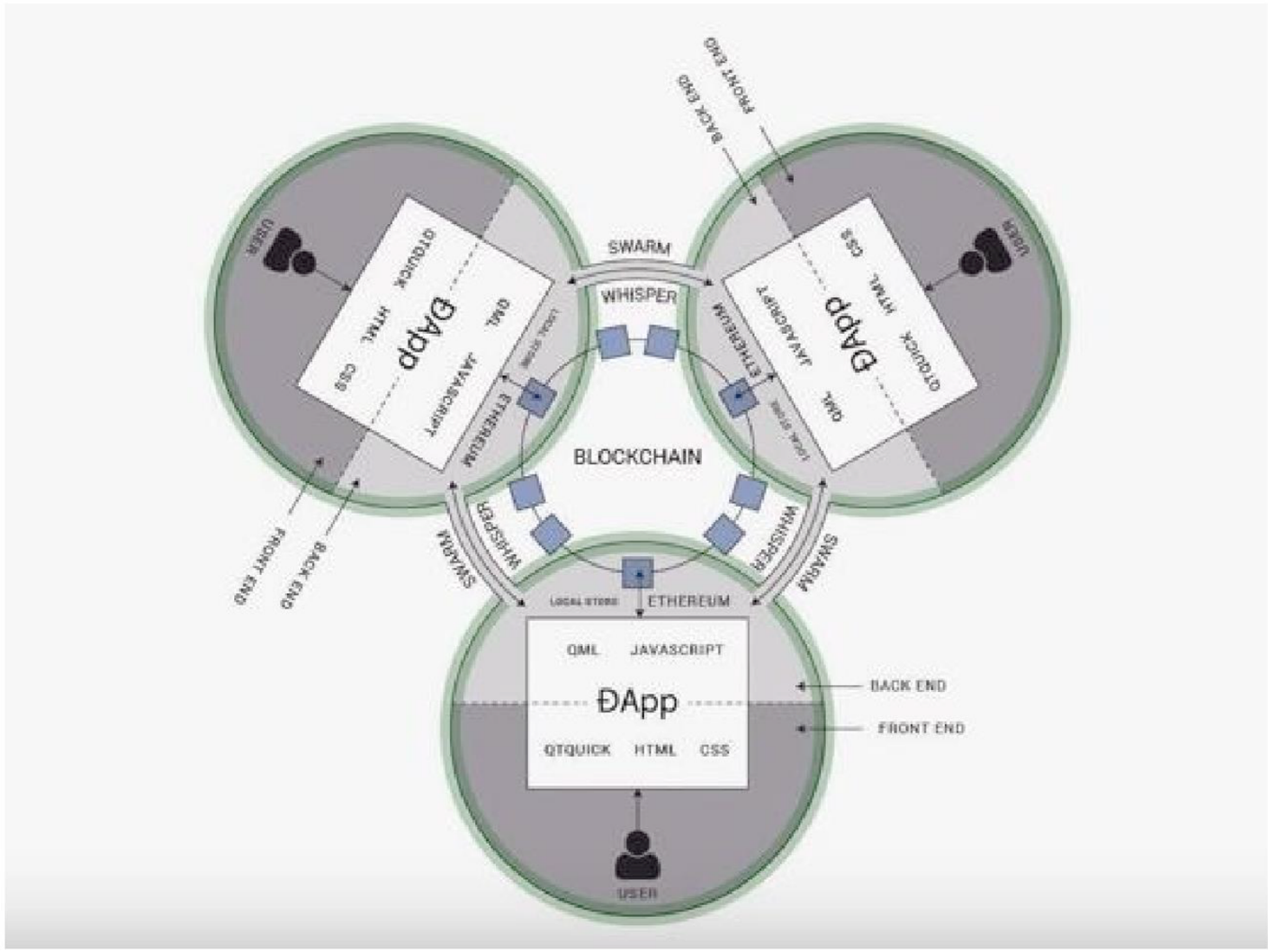
联盟链可以没有币

空气币可以没有链

开源项目

- 公有链
  - 面向公众，人人皆可参与，类比公共互联网
  - 匿名化，多面向完全不可信场景，支持加密货币
  - 比特币（Bitcoin）、以太坊（Ethereum）
- 联盟链
  - 面向企业，联盟成员可参与，类比企业网
  - 实名，访问权限控制，存在一定信任前提
  - 超级账本（Hyperledger）
- 其它有特点的项目
  - Ripple，R3 Corda，IOTA，EOS等

DAPP



https://www.stateofthedapps.com/dapps

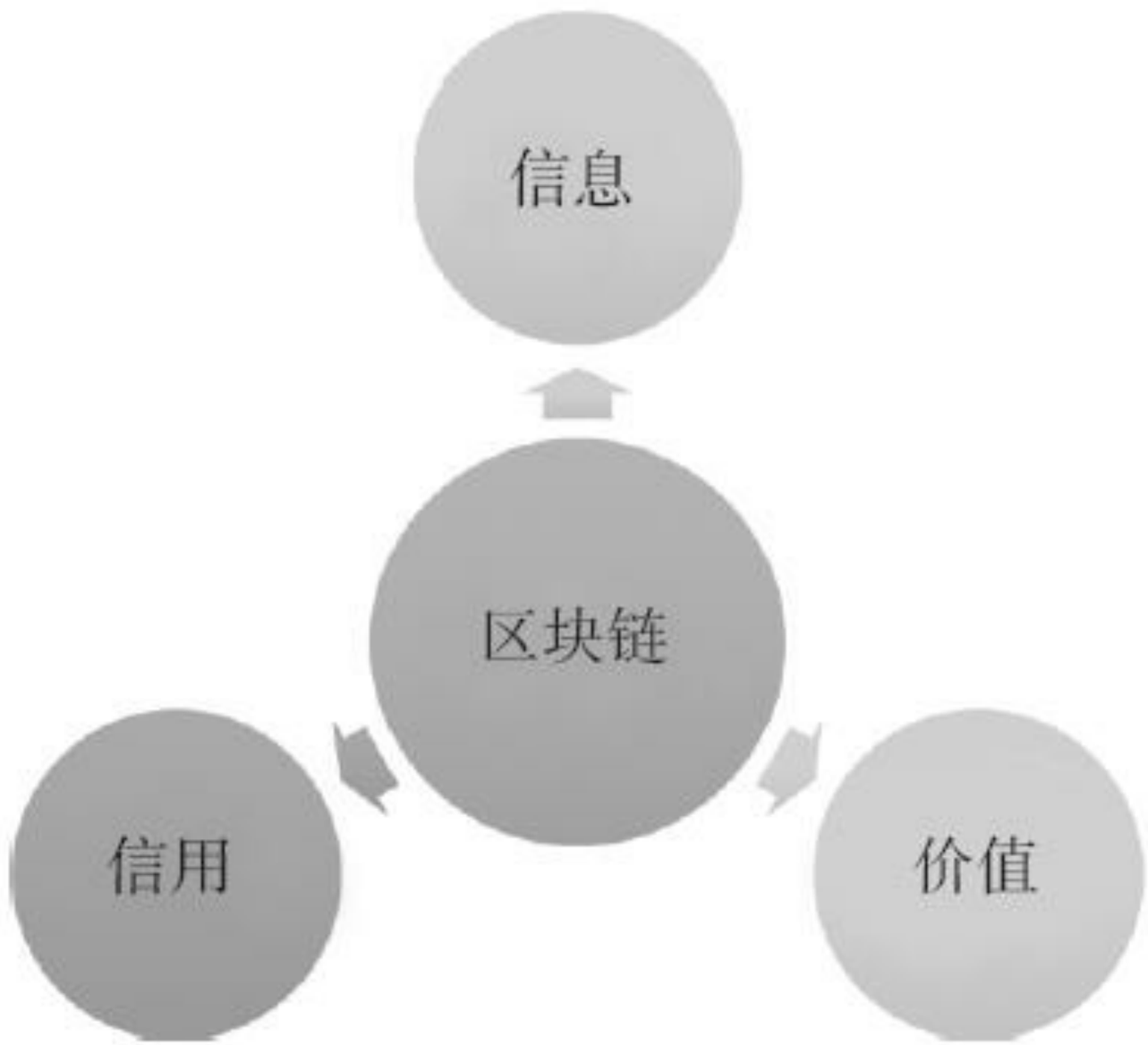
HyperLedger

区块链原理、设计与应用

数字货币和纸币

属性	分　　析	优势方
便携	大部分场景（特别是较大数额支付时）下数字货币将具备更好的便携性	数字货币
防伪	两者各有千秋，但数字货币整体上会略胜一筹。纸币依靠的是各种设计（纸张、油墨、暗纹、夹层等）上的精巧，数字货币依靠的则是密码学上的保障。事实上，纸币的伪造时有发生，但数字货币的伪造目前还无法实现	数字货币
辨伪	纸币即使依托验钞机等专用设备仍会有误判情况，数字货币依靠密码学易于校验	数字货币
匿名	通常情况下，两者都能提供很好的匿名性。但都无法防御有意的追踪	持平
交易	对纸币来说，谁持有纸币谁就是合法拥有者，交易通过纸币自身的转移即可完成，无法复制。对数字货币来说则复杂得多，因为任何数字物品都是可以被复制的，但数字形式也意味着转移成本会更低。总体上看，两者适用不同的情景	持平
资源	通常情况下，纸币的生产成本要远低于面额。数字货币消耗资源的计算则复杂得多。以比特币为例，最坏情况下可能需要消耗接近甚至超过面值的电能	纸币
发行	纸币的发行需要第三方机构的参与，数字货币则通过分布式算法来完成发行。在人类历史上，通胀和通缩往往是不合理地发行货币造成的，而数字货币尚缺乏大规模验证，还有待观察	持平

区块链交换



区块链技术演化

场景	功能	智能合约	一致性	权限	类型	性能	编程语言	代表
公信的数字货币	记账功能	不带有或较弱	PoW	无	公有链	较低	简单脚本	比特币网络
公信的交易处理	智能合约	图灵完备	PoW、PoS	无	公有链	受限	特定语言	以太坊网络
带权限的分布式账本处理	商业处理	多种语言，图灵完备	包括CFT、BFT在内的多种机制，可插拔	支持	联盟链	可扩展	高级编程语言	超级账本

应用领域

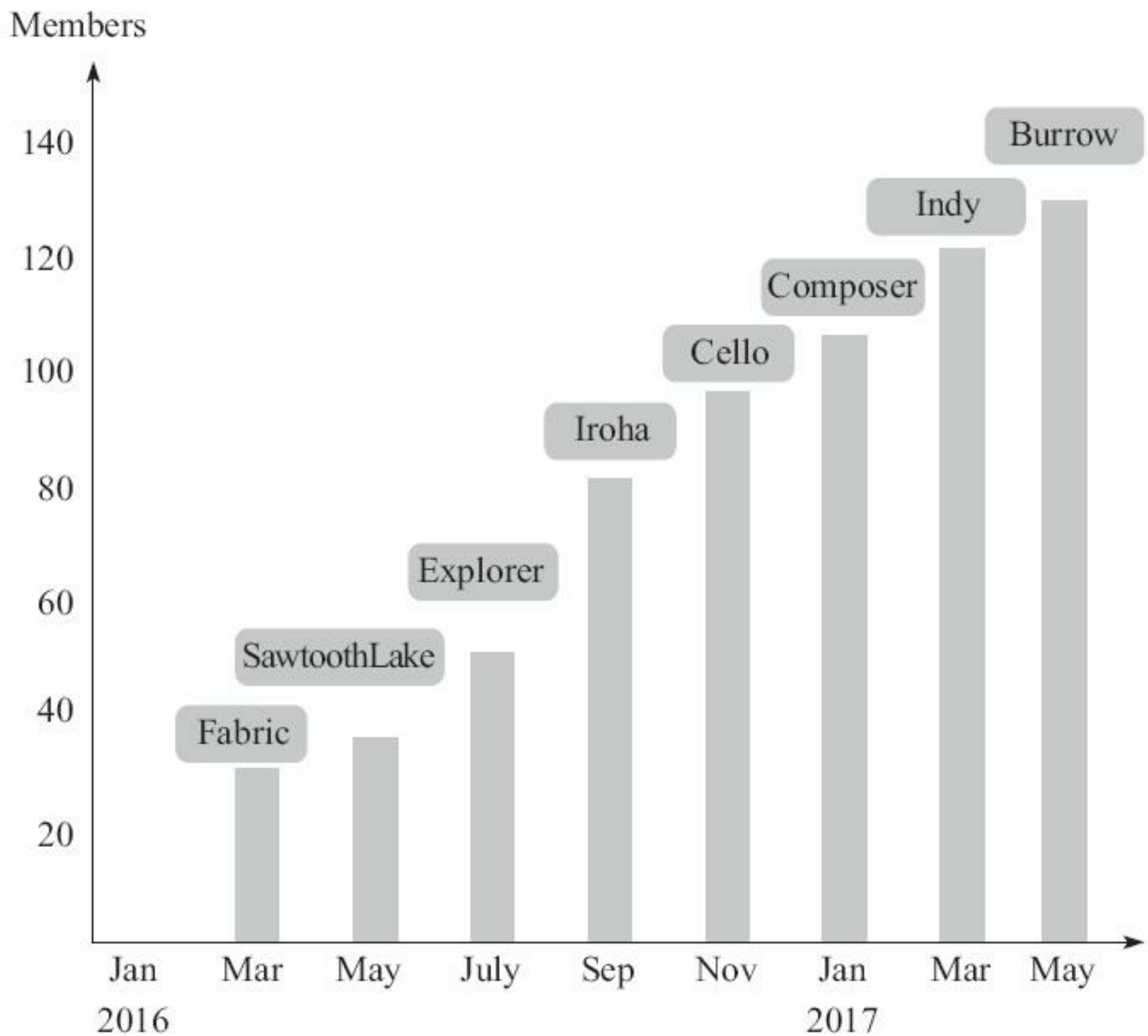
- 数字货币
- 证券交易
- 征信和权属管理
- 资源共享
- 贸易管理
- 物联
- 其他

超级账本

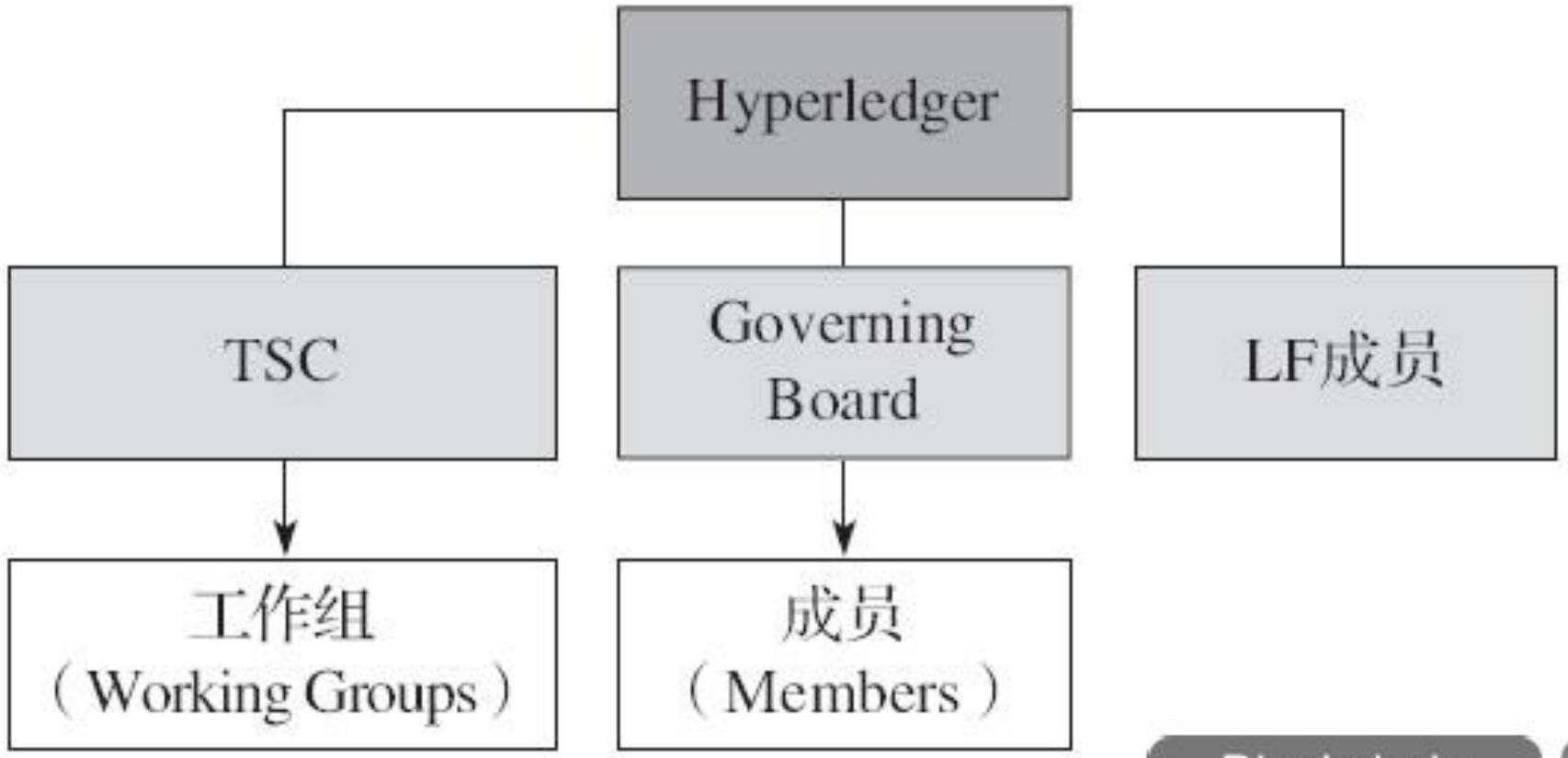
Hyperledger(或Hyperledger项目)是一个旨在推动区块链跨行业应用的开源项目，由Linux基金会在2015年12月主导发起该项目，成员包括金融，银行，物联网，供应链，制造和科技行业的领头羊。

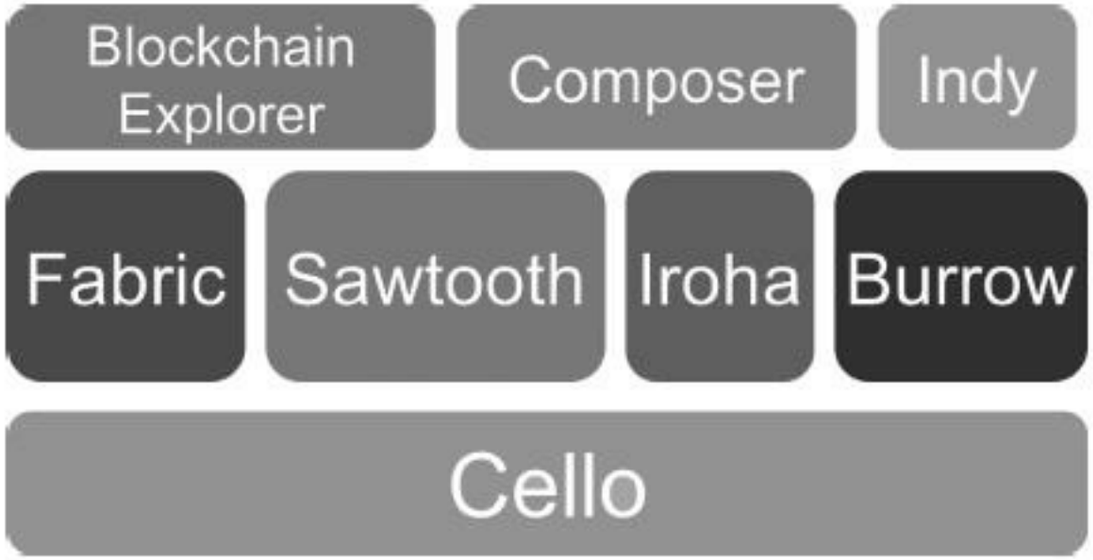
项目的目标是区块链及分布式记账系统的跨行业发展与协作，并着重发展性能和可靠性（相对于类似的数字货币的设计）使之可以支持主要的技术、金融和供应链公司中的全球商业交易。该项目将继承独立的开放协议和标准，通过框架方法和专用模块，包括各区块链的共识机制和存储方式，以及身份服务、访问控制和智能合约。

发展

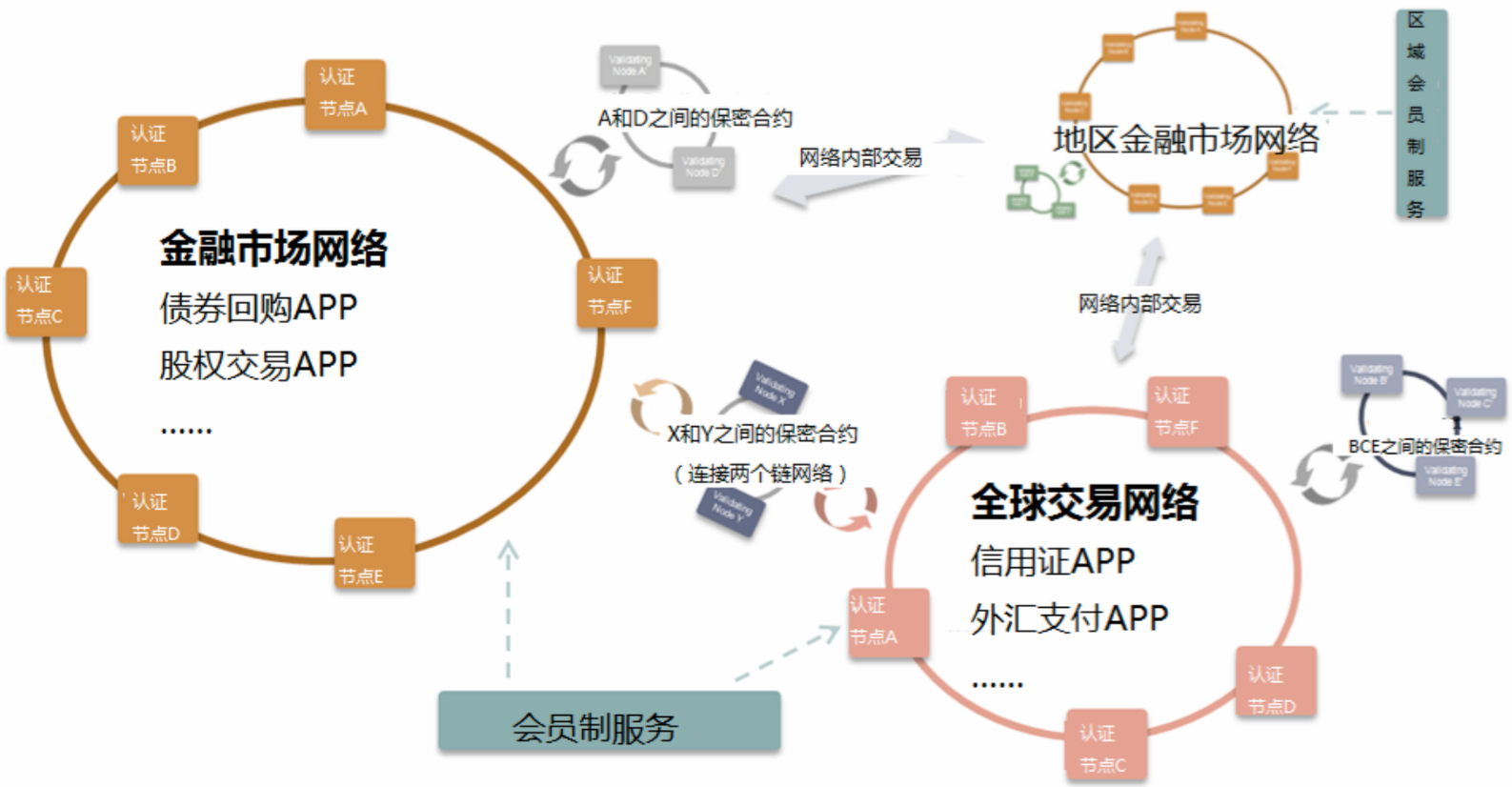

Members
140
120
100
80
60
40
20
Fabric
SawtoothLake
Explorer
Iroha
Cello
Composer
Indy
Burrow
Jan
2016
Mar
May
July
Sep
Nov
Jan
2017
Mar
May

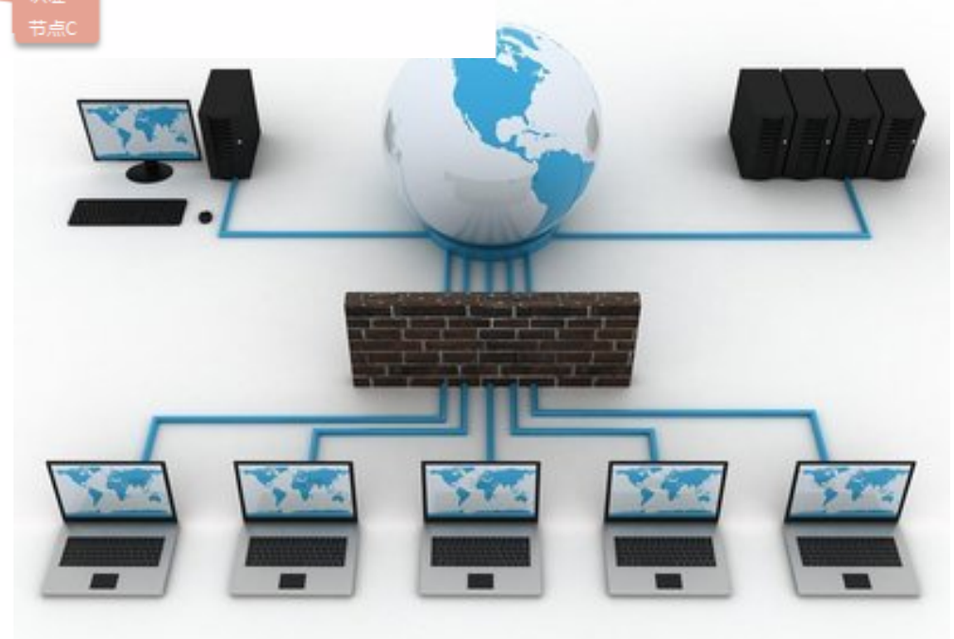
发展


Hyperledger
TSC
Governing Board
LF成员
工作组
（Working Groups）
成员
（Members）

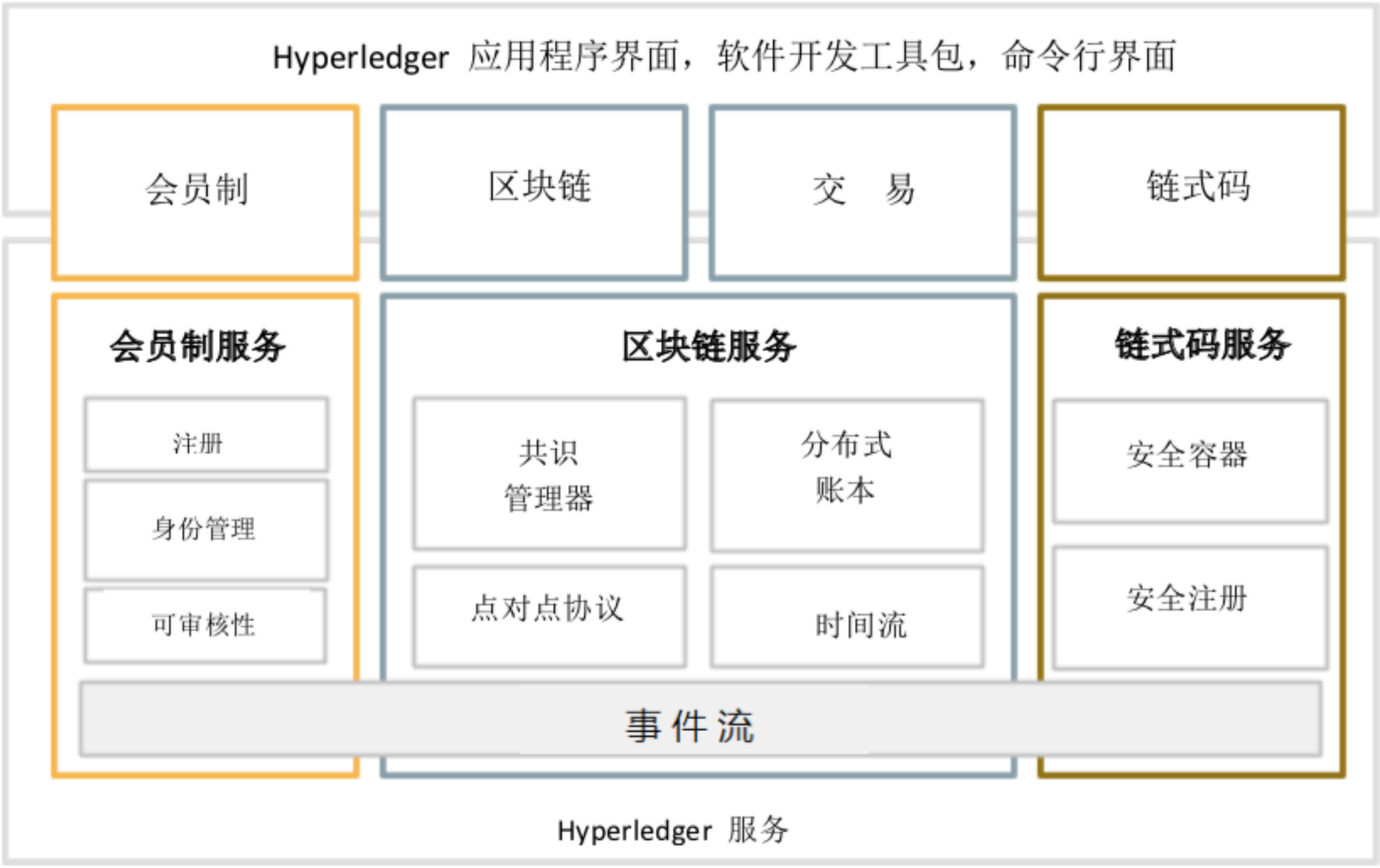

Blockchain Explorer
Composer
Indy
Fabric
Sawtooth
Iroha
Burrow
Cello

HyperLedger 超级账本



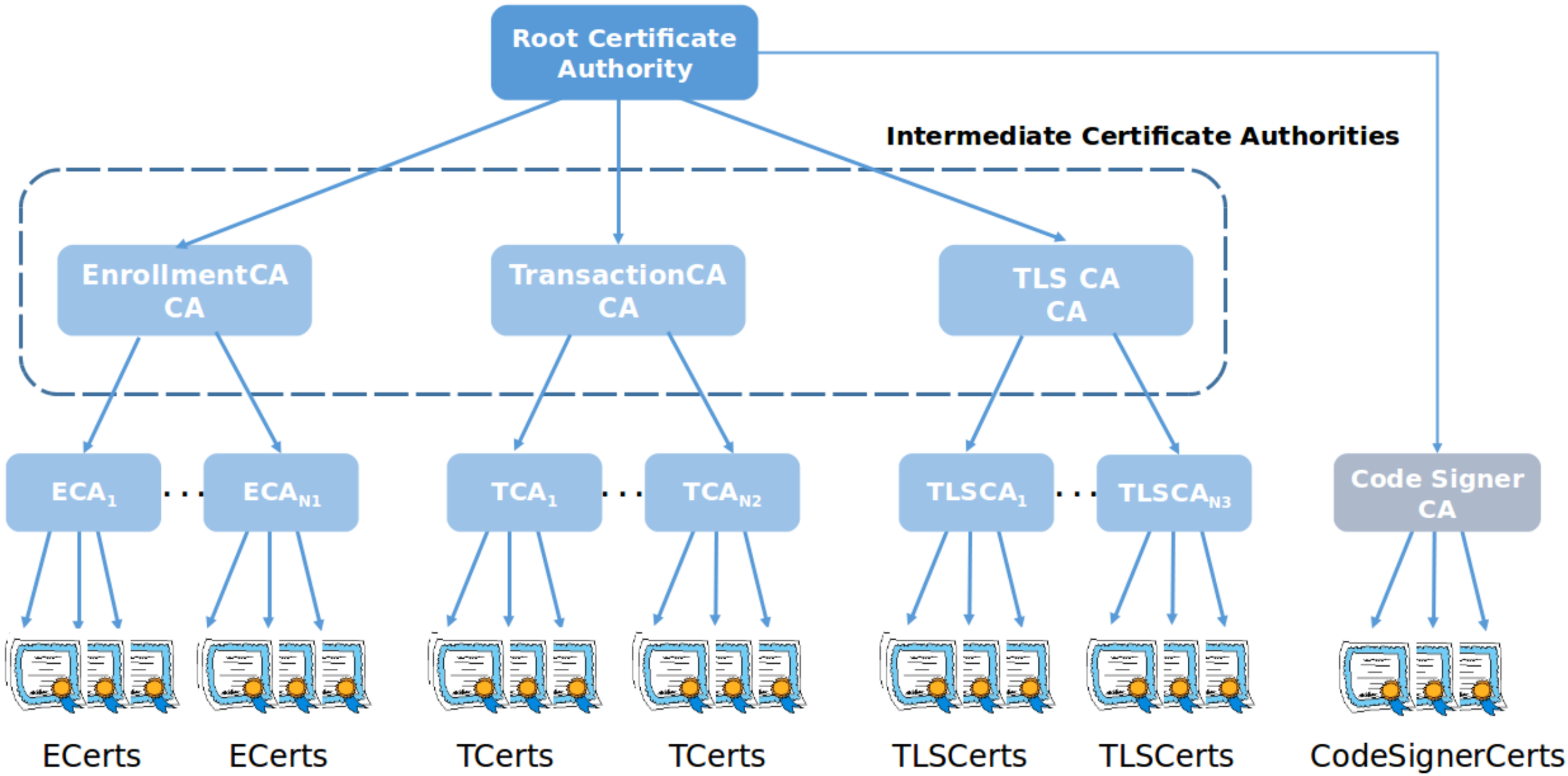


超级账本

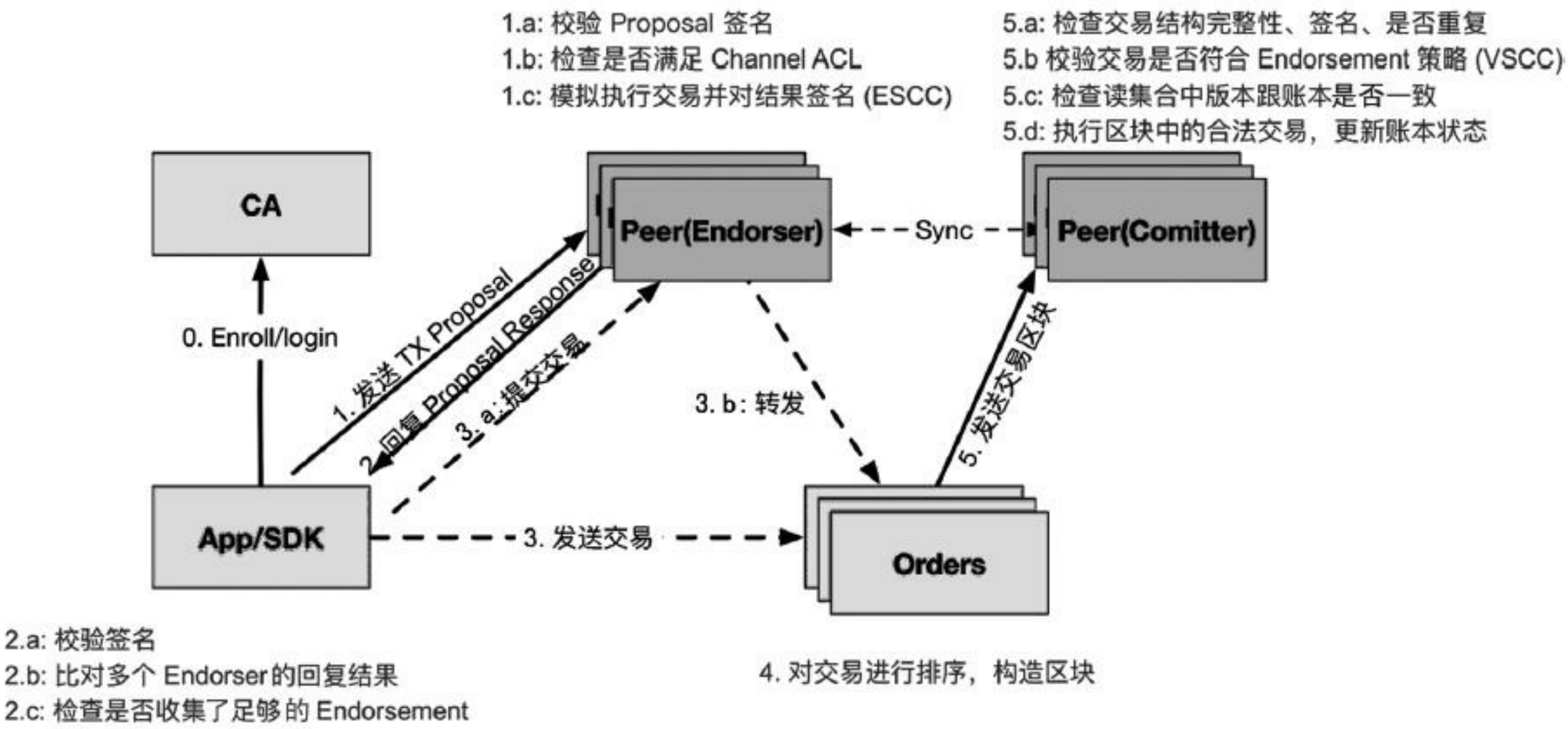

Hyperledger 应用程序界面，软件开发工具包，命令行界面
会员制
区块链
交 易
链式码
会员制服务
注册
身份管理
可审核性
区块链服务
共识
管理器
分布式
账本
点对点协议
时间流
链式码服务
安全容器
安全注册
事件流
Hyperledger 服务

PKI

Public Key Infrastructure – Hierarchy

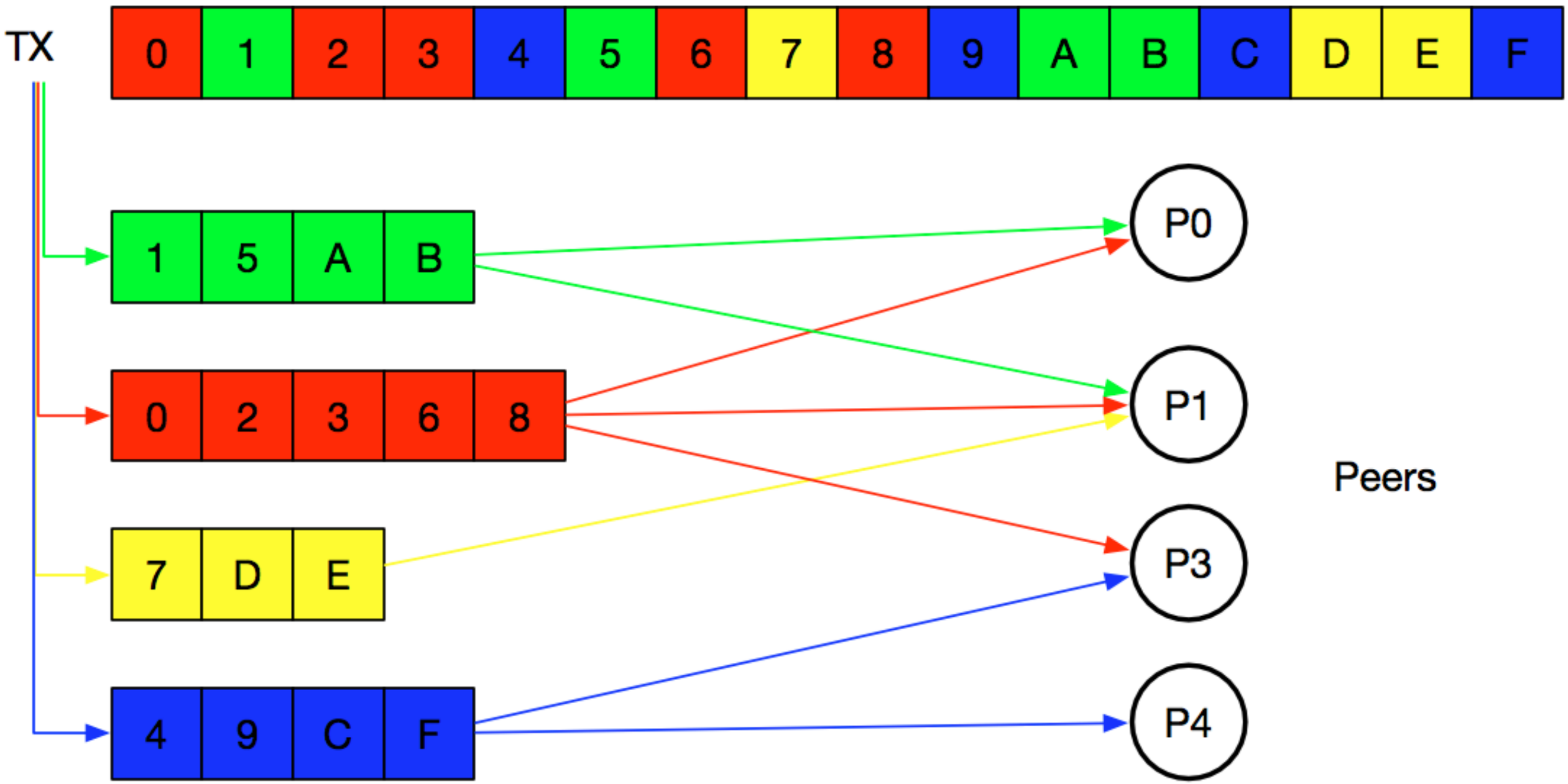


超级账本



TX Proposal: channel id + chaincode + arguments + user signature
Proposal Response: r/w sets + endorsement statement + endorser signature
TX: r/w sets + endorser signatures + channel id

多通道



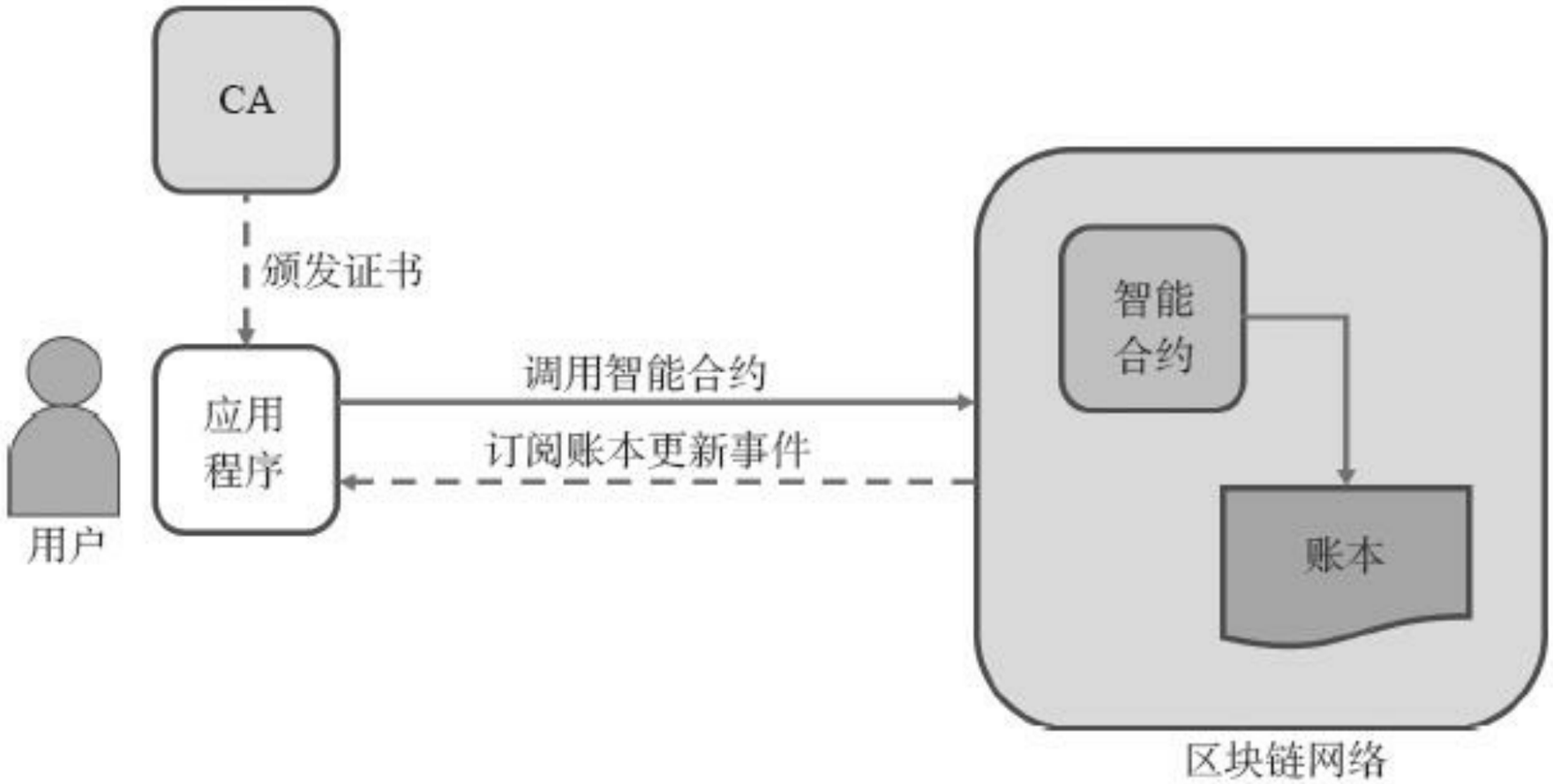
超级账本

业务开发人员

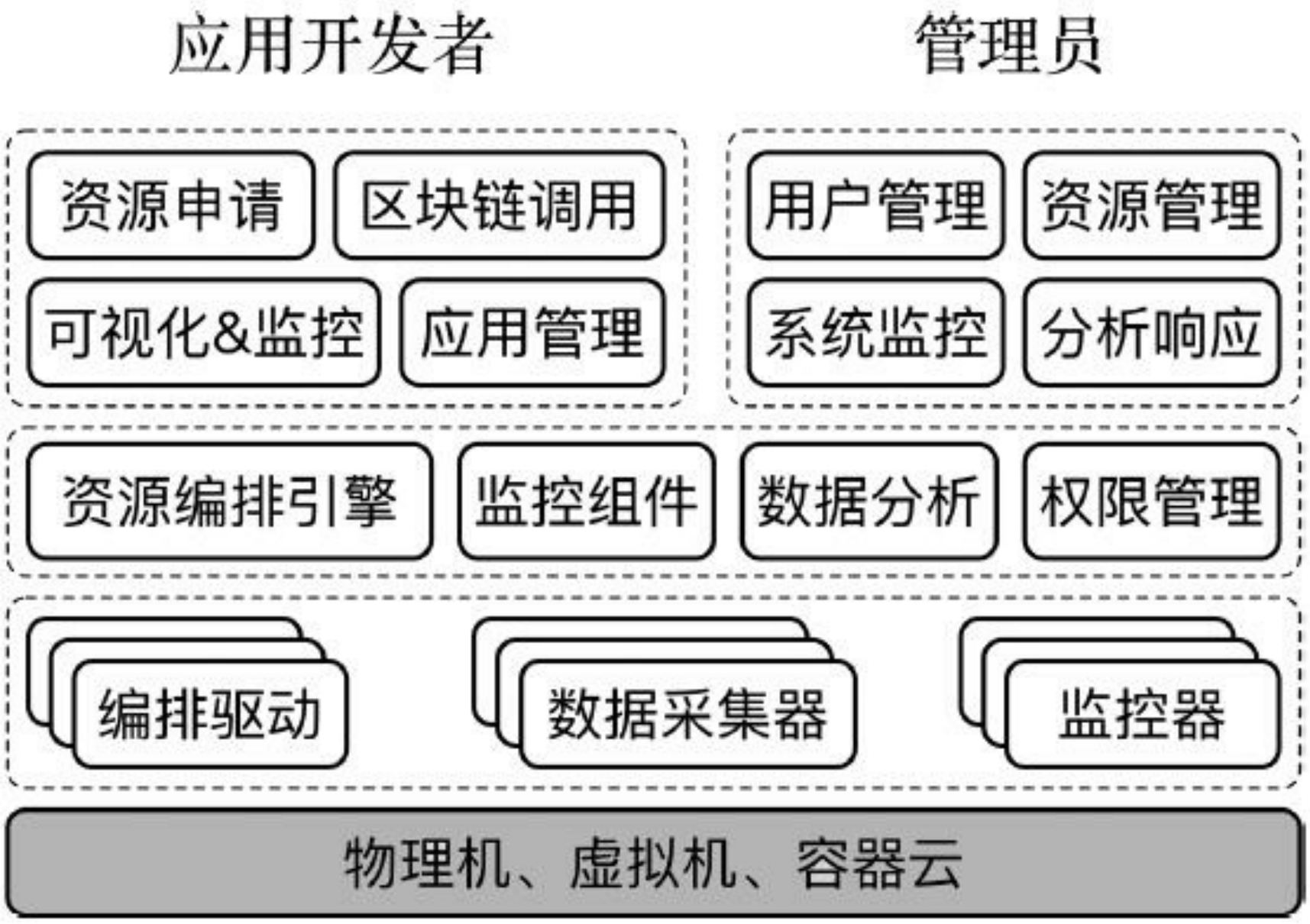
组织管理人员

系统管理人员

应用项目



参考架构


应用开发者
管理员
资源申请
区块链调用
可视化&监控
应用管理
用户管理
资源管理
系统监控
分析响应
资源编排引擎
监控组件
数据分析
权限管理
编排驱动
数据采集器
监控器
物理机、虚拟机、容器云

IPFS

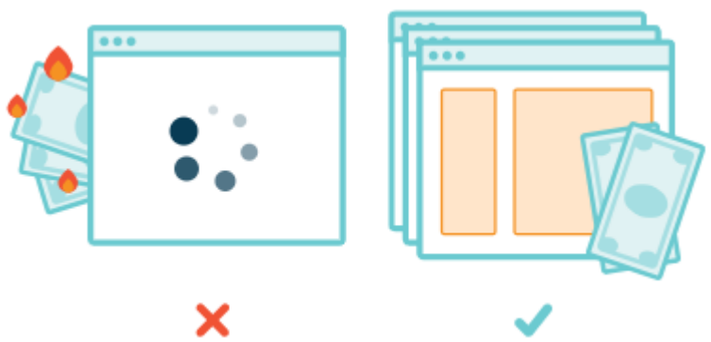
IPFS

IPFS:星际文件系统(InterPlanetary File System)

- 本质上是一种内容可寻址、版本化、点对点超媒体的分布式存储、传输协议
- 目标是补充乃至取代过去20年里使用的超文本媒体传输协议（HTTP），创建分布式Web，希望构建更快、更安全、更自由开放的互联网时代
- Ipfs最核心的技术是p2p，原来是中心化的服务器在分发内容，而IPFS模式下想要下载某一个内容，可同时从多个对等实体获取内容

IPFS旨在代替HTTP，为人类创建一个更好的web

IPFS: 为何需要



HTTP低效且成本高

历史数据经常被删除

中心化限制了web的成长

互联网应用高度依赖互联网主干网

IPFS发展

- 2014年5月，Juan Benet发起IPFS项目
- 2015年年1月，IPFS协议实验室成立，并发布IPFS
- 2016年，IPFS团队创建了了libp2p、IPLD、multiformats、Orbit等模块
- 2017年年6月，IPFS已储存50亿份文件
- 2017年年7月，IPFS团队宣布成立立Filecoin项目
- Filecoin项目预计于2018年底上线（已跳票）

IPFS如何工作

每一个文件和组成文件的文件块有一个加密指纹

IPFS在整个网络范围内去掉重复的文件

如果仅仅使用哈希值来区分文件的话，会给传播造成困难，因为哈希值不容易记忆，就像ip地址一样不容易记忆，于是人类发明的域名。IPFS利用IPNS将哈希值映射为容易记的名字

当查询文件的时候, IPFS网络根据文件的哈希值(全网唯一)进行查找。 由于每个文件的哈希值全网唯一, 查询将很容易进行

IPFS基本知识

- 分布式哈希表(DHT)

➢ 是分布式计算系统中的一类，可由键值来唯一标示的信息按照某种约定/协议被分散地存储在多个节点上，这样也可以有效地避免“中央集权式”的服务器的单一故障而带来的整个网络瘫痪。实现DHT的技术/算法有很多种，常用的有：Chord, Pastry, Kademlia等

- 块交换 – BitTorrent

➢ 一种点对点传输的网络协议。常见的BT软件有：迅雷、QQ旋风、比特精灵等

- 版本控制系统- Git

➢ Git(版本化)实现了文件的历史版本控制器，并且让多节点使用保存不同版本的文件

- 自我认证认文件系统-SFS

➢ 实现了分布式信任链、平等共享的全局命名空间

IPFS架构

IPFS协议栈

身份	S/Kademlia生成，对等身份信息生成
网络	任意传输层协议，ICE NET & NAT穿透
路由	分布式松散哈希表（DSHT），定位对等点和存储对象需要的信息
交换	BitTorrent& BitSwap，管理区块如何分布
对象	Merkle-DAG，内容可寻址的不可篡改、去冗余的对象链接
文件	类似Git版本控制的文件系统：blob,list, tree, commit
命名	具有SFS（Self-CertifiedFilesystems）IPNS：DAG对象命名可变
应用	在IPFS上运行的应用程序利用最近节点提供服务提供效率、降低成本

IPFS身份层

- 对等节点身份信息的生成以及路由规则是通过Kademlia协议生成制定，KAD协议实质是构建了一个分布式松散Hash表（distributedhash table），简称DHT，每个加入这个DHT网络的人都要生成自己的身份信息，然后才能通过这个身份信息去负责存储这个网络里的资源信息和其他成员的联系信息
S/Kademlia生成NodeId:

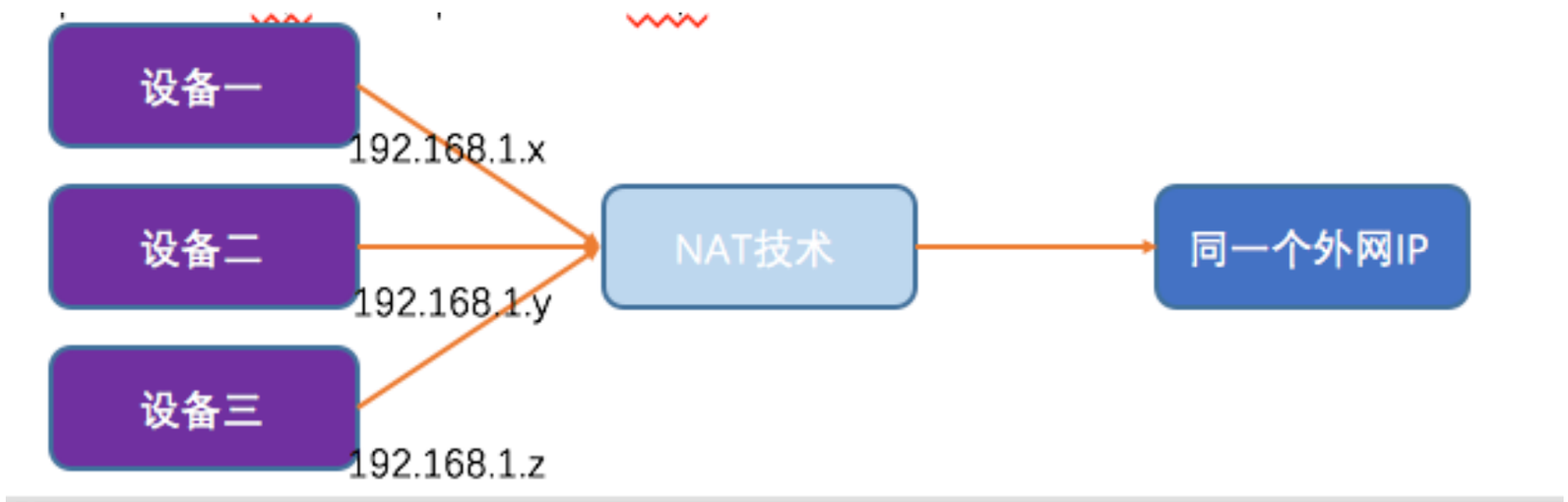
```
  difficulty = <integer parameter>n = Node{}do {
n.PubKey, n.PrivKey = PKI.genKeyPair()
n.NodeId = hash(n.PubKey)
p = count_preceding_zero_bits(hash(n.NodeId))} while (p < difficulty)
```

- 每一个节点在 IPFS 代码中都由`Node` 结构体来表示，其中只包含 `NodeId` 以及一个公私钥对
- 身份系统的主要作用就是表示 IPFS 网络中的每一个节点，代表每一个使用 IPFS 的用户

IPFS网络层

- LibP2P可以支持任意传输层协议。ICE NAT traversal框架整合STUN、TURN和其他类型的NAT协议，该框架可以让客户端利用各种NAT方式打通网络，从而完成NAT通信，这对于IPFS的p2p网络非常重要
- IPFS 可以使用任意的网络进行通信，它并没有假设自己一定运行在 IP 协议上，而是通过 multiaddr 的格式来表示目标地址和使用的协议，以此来兼容和扩展未来可能出现的其他网络协议：

/ip4/10.20.30/40/sctp/1234/
/ip4/5.6.7.8/tcp/5678/ip4/1.2.3.4/sctp/1234/

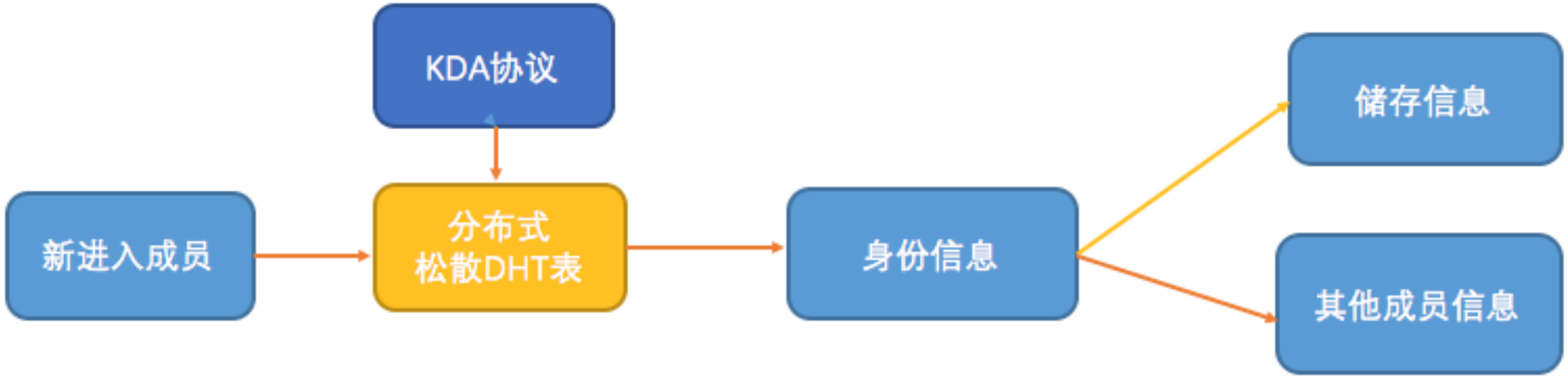


IPFS路由层

在一个分布式系统中，检索或者访问其他节点中存储的资源就需要通过一个路由系统，IPFS 使用了基于 S/Kademlia 和 Coral 中的 DSHT 实现了路由系统

IPFS 中的路由需要实现三种基本的功能，内容路由、节点路由以及数据存储。实现了这几些接口的路由器就可以在底层进行替换，不会影响系统其他部分的工作。目前 IPFS 使用全局 DHT 和 DNS 来解析路由记录，而 Kademlia DHT 有以下的优点：

1. 在批量节点中快速找到目标地址，时间复杂度是 $\log_2(n)$，也就是说，在10,000,000节点中只需要20次查询；
2. 优化了节点之间的控制消息长度，降低了信息协调的开销；
3. 通过优先选择长期节点抵御多种网络攻击；
4. 在点对点的应用中被广泛应用，例如 BitTorrent 和 Gnutella，技术也比较成熟；



IPFS数据交换

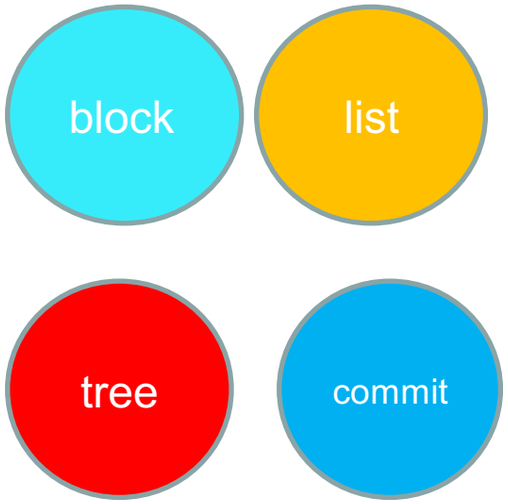
- 类似迅雷这样的BT工具，IPFS团队把BitTorrent进行了创新，叫作Bitswap。BitSwap 负责两件事情：向其他节点请求需要的 Block 以及为其他节点提供 Block
- 当我们需要向其他节点请求 Block 或者为其他节点提供 Block 时，都会发送 BitSwap 消息，其中主要包含了两部分内容：发送者的 wantlist以及数据块
- 增加了信用和帐单体系来激励节点去分享，用户在发送给其他节点数据可以增加信用值，从其他节点接受数据降低信用值。如果用户只去接收数据而不分享数据，信用分会越来越低而被其他节点忽略掉
- 负债比率是用来衡量节点之间信任的，它不仅能够阻止攻击者创建大量的节点、还能在节点短时间不可用时保护已有的交易关系并且在节点关系恶化之前终止交易

$$r = \frac{bytes_sent}{bytes_recv + 1}$$

IPFS对象层和文件层

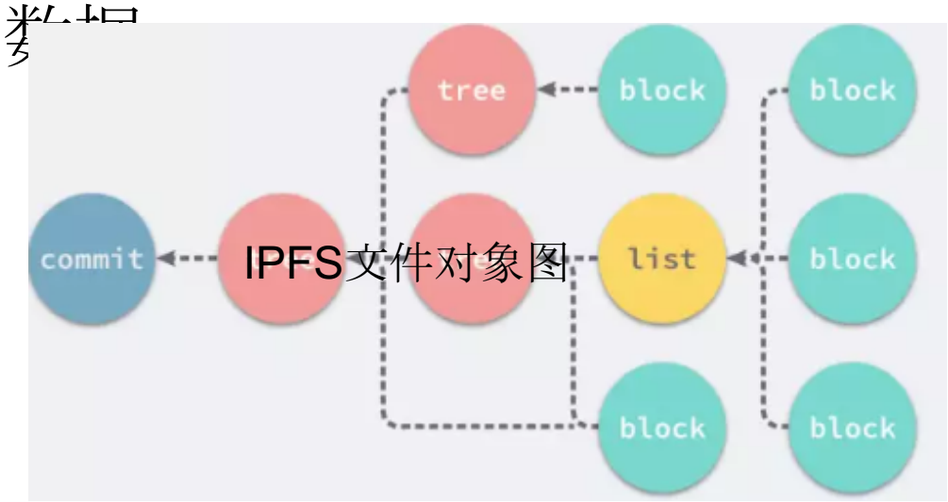
- DHT 和 BitSwap 允许 IPFS 构建一个用于存储和分发数据块的大型点对点系统；在这之上，IPFS 构建了一个 Merkle DAG，每一个 IPFS 对象都可能包含一组链接和当前节点中的数据

IPFS对象模型



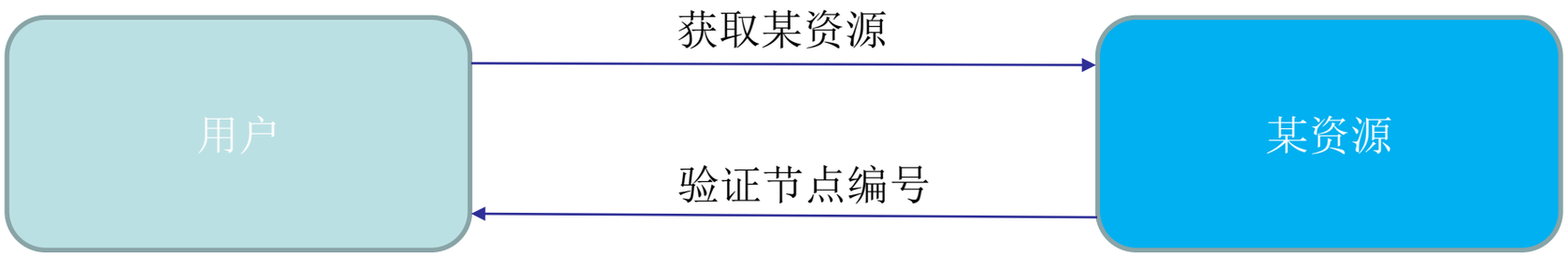
IPFS 文件可以通过 list和blob 进行表示：

- 其中 blob不包含任何的链接，只包含数据；
- 但是 list却包含了一个 blob 和 list的有序队列；
- 而 tree文件对象与 Git 中的tree 非常相似，它表示一个从名字到哈希的文件目录；
- 最后的 commit 表示任意对象的快照；



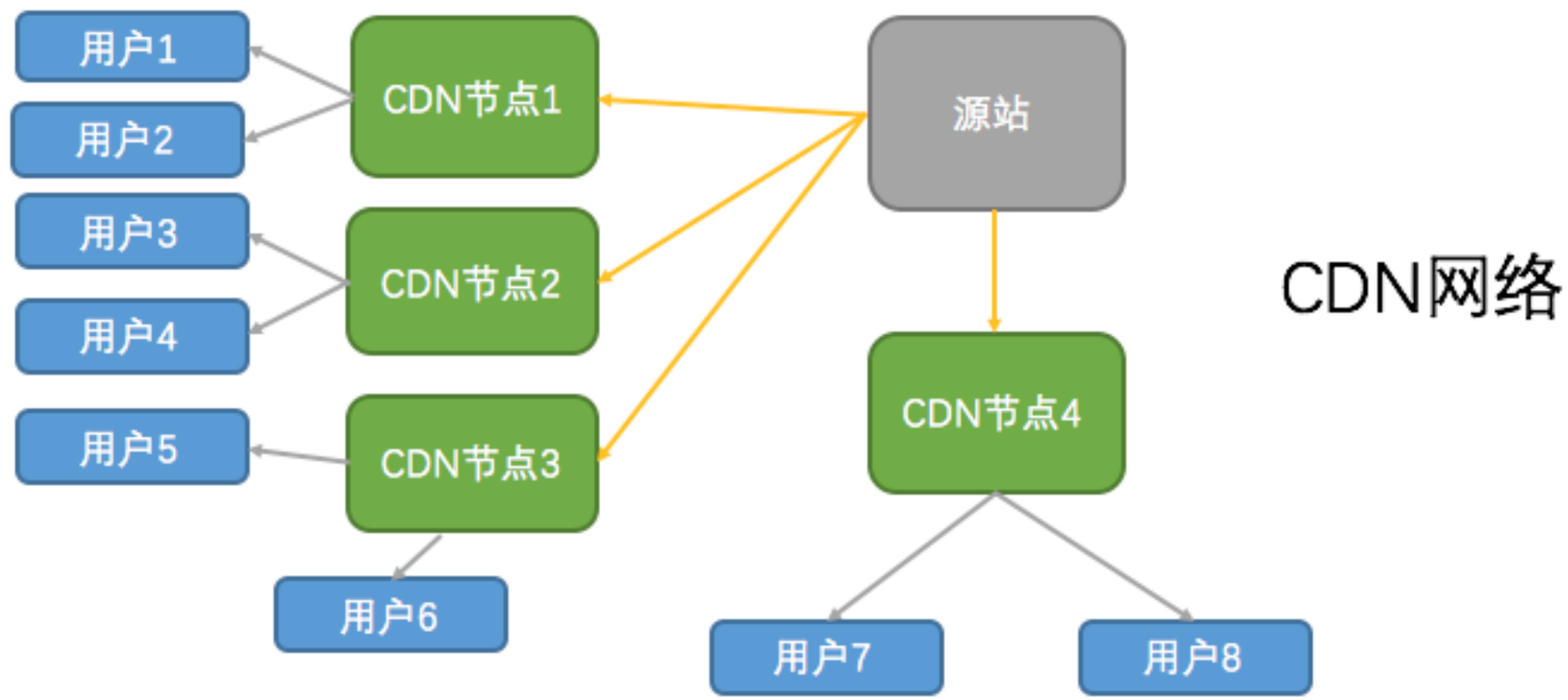
IPFS命名层

- 可变的命名系统也是网络不可缺少的一部分，需要使用同一个地址获取不同的状态，因为不能因为网站的更新而改变域名，所以 IPFS 需要提供一种域名服务解决这一问题。
- 在 IPFS 中可以使用IPNS可变命名空间来解决这些问题，用户可以发布一个对象，其他节点就可以通过 ipns 加上该用户的节点地址访问到这些发布到网络中的对象
- 命名层具有自我验证的特性,当其他用用户获取该对象时，使用指纹公钥进行验签，即验证所用的公钥是否与NodeId(节点编号）匹配，这验证了用户发布对象的真实性



IPFS价值

IPFS核心价值就在于上面运行的应用程序，可以利用它类似CDN的功能，在成本很低的带宽下，去获得想要的数据，从而提升整个应用程序的效率



IPFS家族

- IPFS项目其实很大，并不是一个东西，IPFS是由很多模块组成，每一个模块现在都已经独立成项目了，并且有自己的主页。
- 协议实验室的主页：https://protocol.ai/projects/
- 在协议实验室的主页上面，可以找到目前的五个项目，来简单看一下IPFS家族成员

Filecoin

- IPFS只是一个协议, 并不是挖矿软件本身。Filecoin系统才是挖矿软件本身, 代币名字是 FIL。Filecoin使用了IPFS 协议来运行系统。Filecoin是IPFS激励层

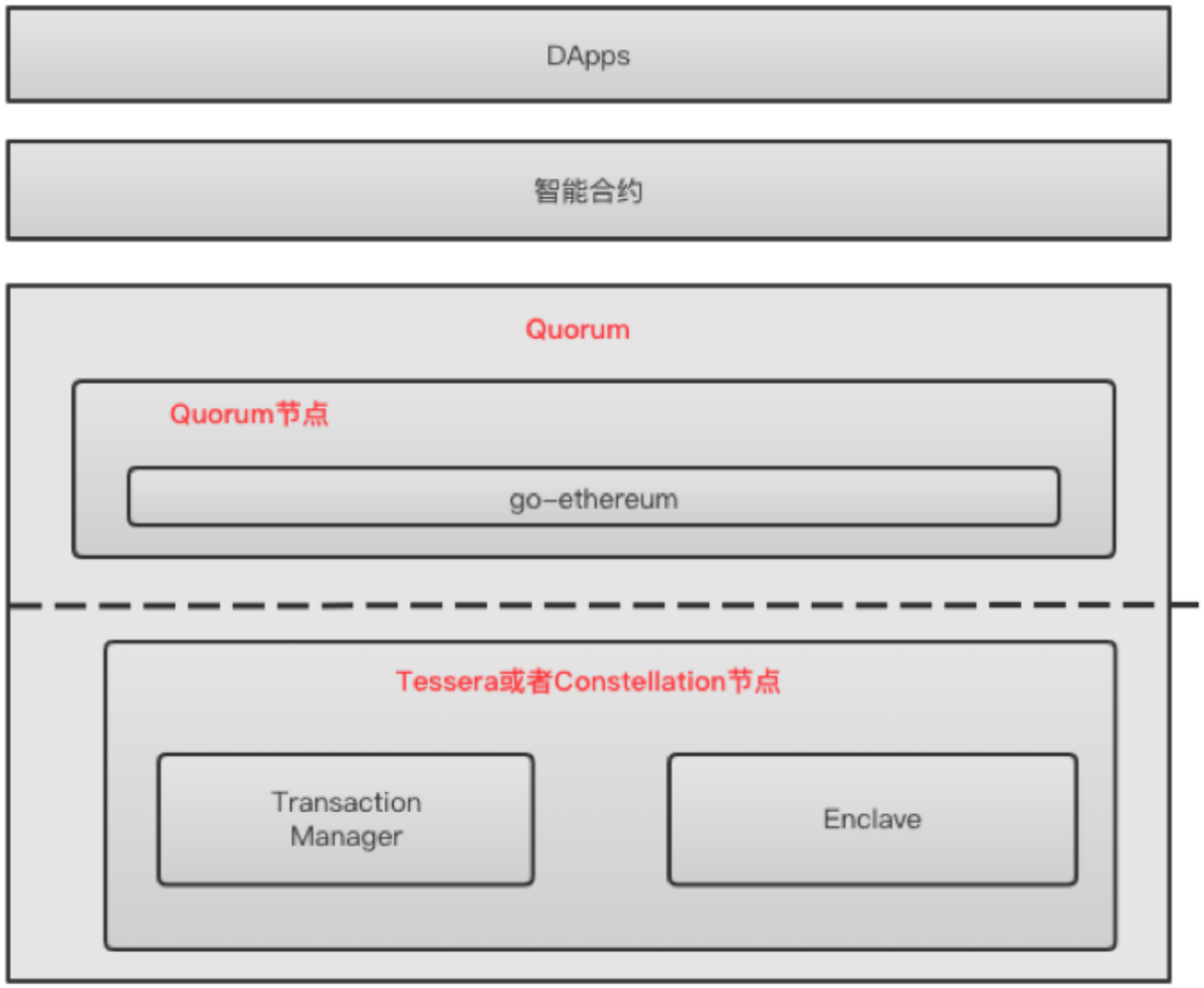
- FIL代币总共有20亿枚。分配方案，总共有四个部分组成：
  - 70%作为挖矿的回报：像比特币一样根据挖矿的进度逐步分发
  - 15%预留Protocol Labs：作为研发费用, 6年逐步解禁
  - 10%分配给ICO投资者：根据挖矿进度, 逐步解禁
  - 5%预留给Filecoin基金会：作为长期社区建设, 网络管理等费用，6年逐步解禁

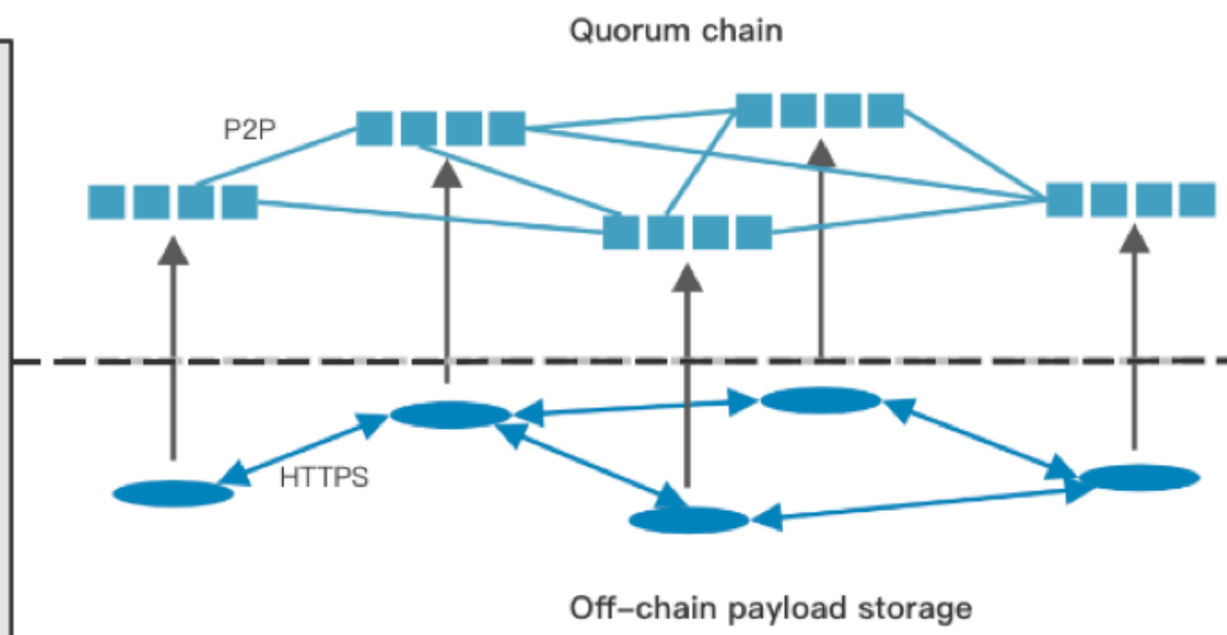
Filecoin证明

- 存储证明（Proof-of-Storage，PoS）：利用存储空间进行的证明。工作量证明的一种，Filecoin上一篇论文使用了这个名字，新的论文则升级为PoRep
- 复制证明（Proof-of-Replication，PoRep）：新的PoS（Proof-of-Storage），PoRep可以保证每份数据的存储都是独立的，可以防止女巫攻击，外源攻击和生成攻击
- 空间证明（Proof-of-Space，PoSpace）：Filecoin提出的概念，存储量的证明，PoSpace是PoW的一种，不同的是PoW使用的计算资源，而PoSpace使用的是存储资源
- 时空证明（Proof-of-Spacetime，PoSt)：时空证明，矿工证明自己花费了spacetime资源,即：一定时间内的存储空间的使用，PoSt是基于PoReps实现的

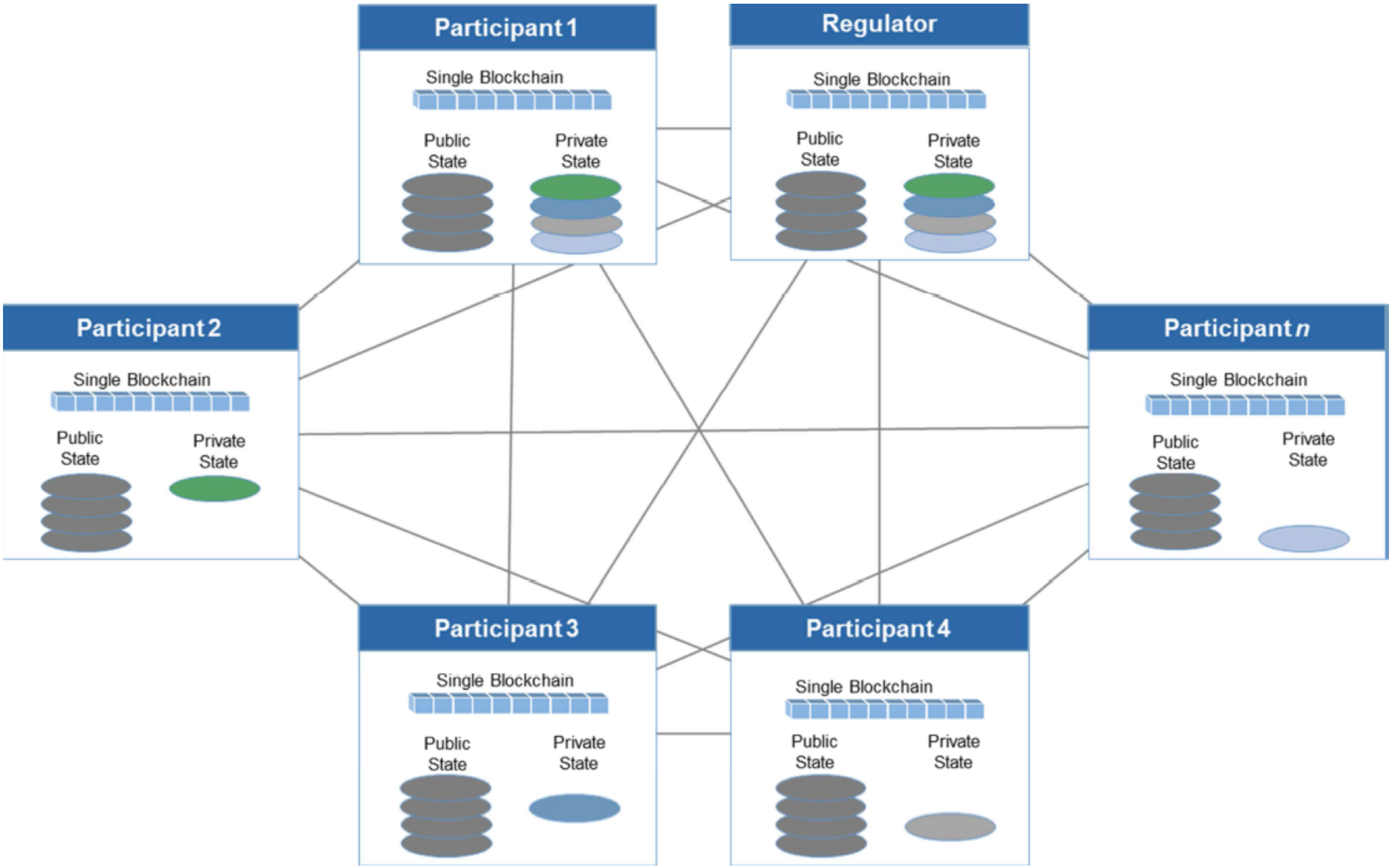
Quorum

Quorum


DApps
智能合约
Quorum
Quorum节点
go-ethereum
Tessera或者Constellation节点
Transaction Manager
Enclave


Quorum chain
P2P
HTTPS
Off-chain payload storage

Quorum

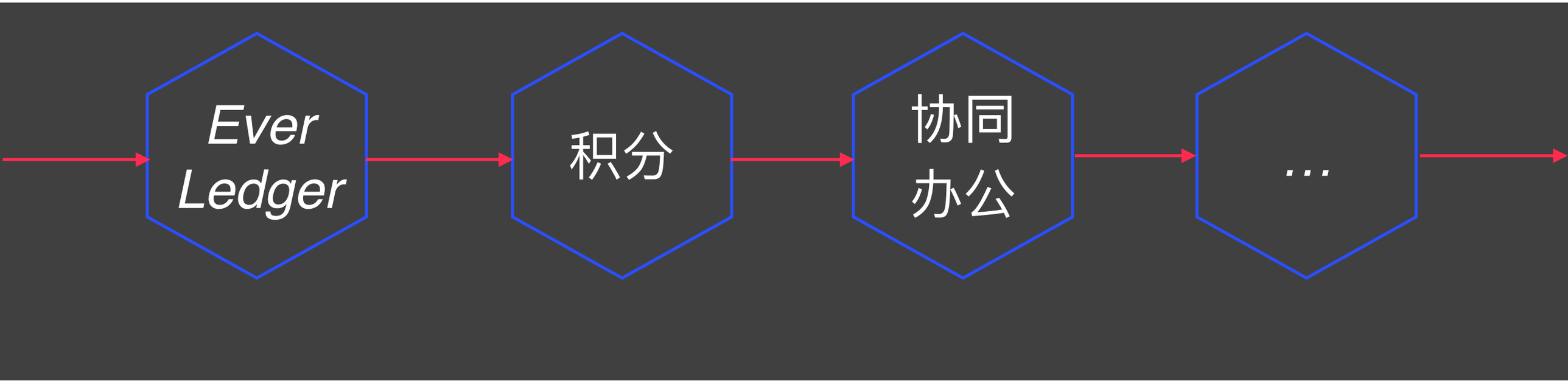

Participant 1
Single Blockchain
Public State
Private State
Regulator
Single Blockchain
Public State
Private State
Participant 2
Single Blockchain
Public State
Private State
Participant n
Single Blockchain
Public State
Private State
Participant 3
Single Blockchain
Public State
Private State
Participant 4
Single Blockchain
Public State
Private State

Quorum

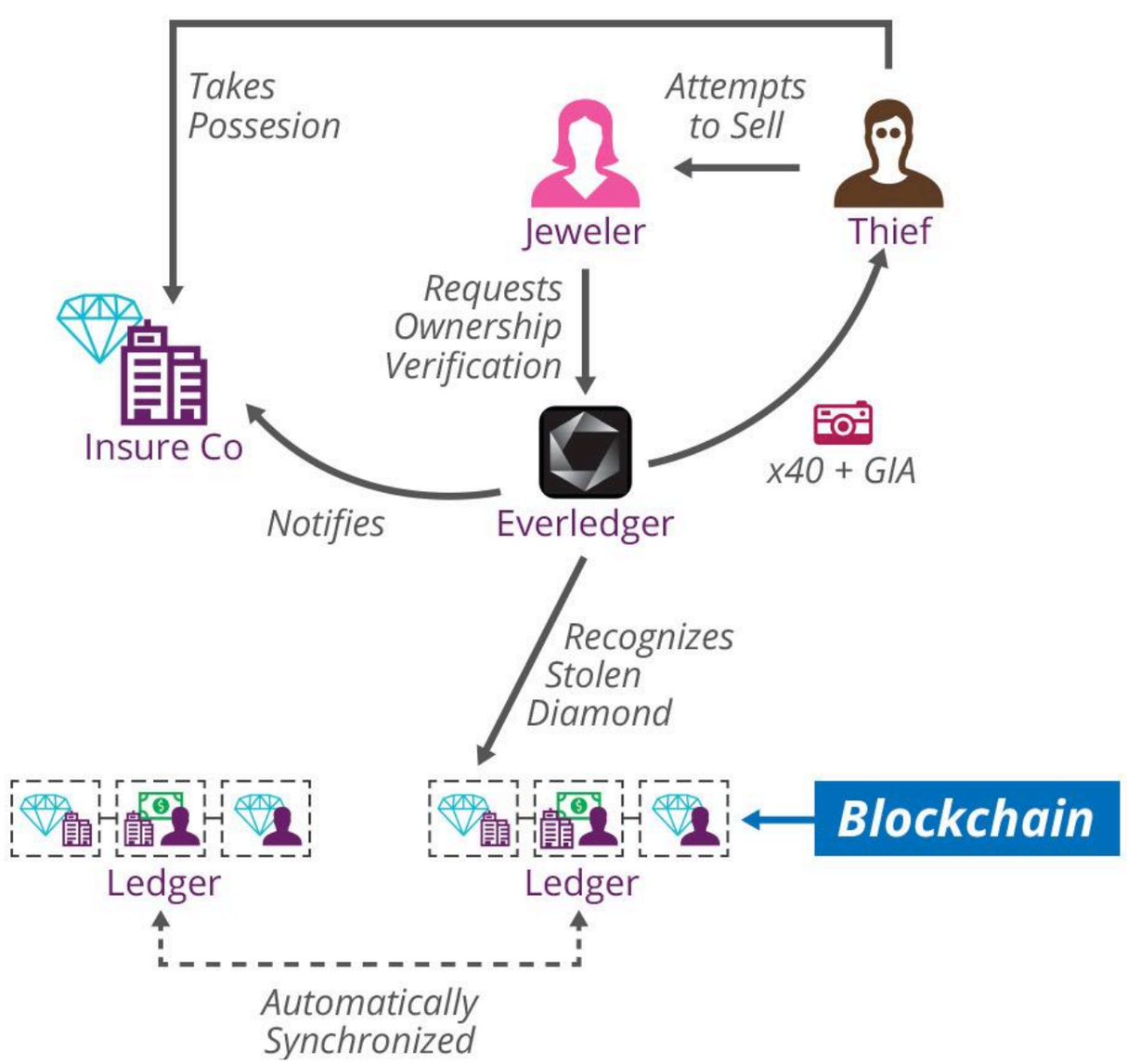
Quorum 组件基于 go-ethereum 修改：

- 共识算法，增加 Raft 和 IBFT 共识
- P2P 网络层，改成只有授权节点才能连入或连出网络
- 区块生成逻辑，由检查“全局状态根”改为检查“全局公开状态根”
- 区块验证逻辑，在区块头，将“全局状态根”替换成“全局公开状态根”
- 状态树，分成公开状态树和私有状态树
- 区块链验证逻辑，改成处理“私有事务”
- 创建事务，改成允许交易数据被加密哈希替代，以维护必需的隐私数据
- 删除以太坊中 Gas 的定价，尽管保留 Gas 本身

区块链应用



EverLedger



商界很早就看到了这项技术所带来的潜力。分布式账本提供了一种确保商品及知识产权的所有权和起源的新方法。例如，Everledger 提供了一种确保钻石身份的分布式账本，并记录从采掘、切割、销售和承保的相关信息。在这个有相对多的纸质文件被伪造的市场里，这种技术让钻石的归类更加高效，并有潜力降低诈骗的风险，以及防止“血腥钻石”（译者注：即在战乱或冲突地区开采并用于资助战争活动的钻石贸易）进入市场。

区块链积分

1 Alice buys airline tickets from Los Angeles to Miami using her credit card

- Alice gets her tickets
- Her credit card transfers loyalty tokens to Alice's loyalty rewards programs digital wallet
- The airline transfers loyalty tokens to her wallet

→

- Alice gains current asset
- The airline and credit card company have current liabilities

2 Alice checks into a major hotel (a national chain) in Miami and realizes she can use points accumulated earlier

- Alice checks into a chain hotel and uses her credit card points to upgrade to a suite
- She also uses her airline points to hire a hotel limousine and posts pictures on social media

→

- Alice has a fantastic experience
- The airline's and credit card company's liabilities are partly cleared while the hotel gets free advertising and a brand advocate

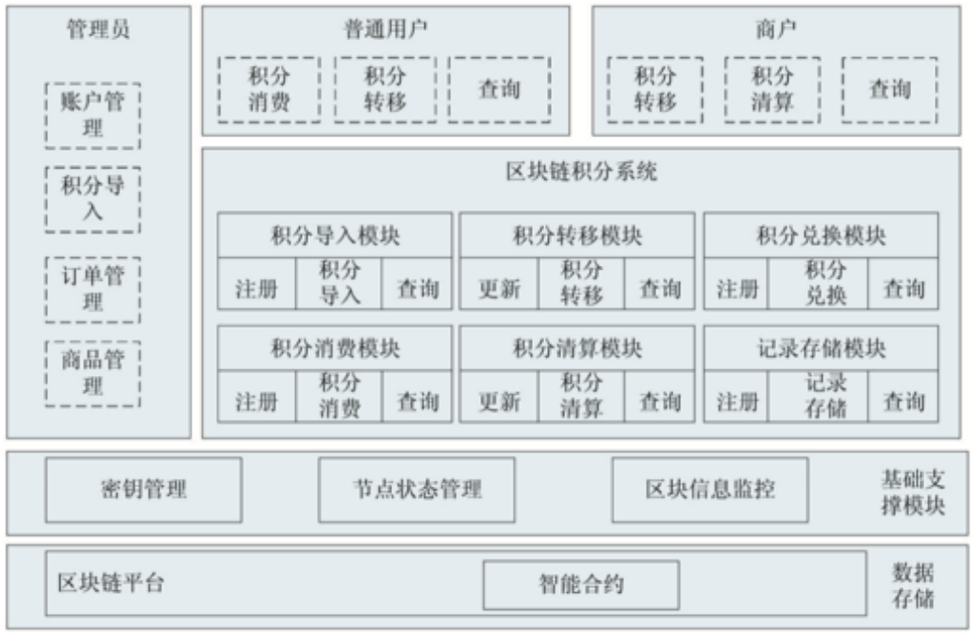
3 Alice meets Bob who wants to hop onto the last flight of the day to LA after missing a flight with another airline

- Alice transfers her airline points to Bob in exchange for his points earned from the hotel chain
- She uses them to extend her holiday while Bob gets a discounted ticket back to LA
- Liability is cleared from the airline's books as the points have been completely used

→

- Alice gets an extended holiday while Bob gets a timely, discounted flight
- Liabilities cleared from the airline's books while the hotel and airline get a happier and new customer, respectively

区块链积分



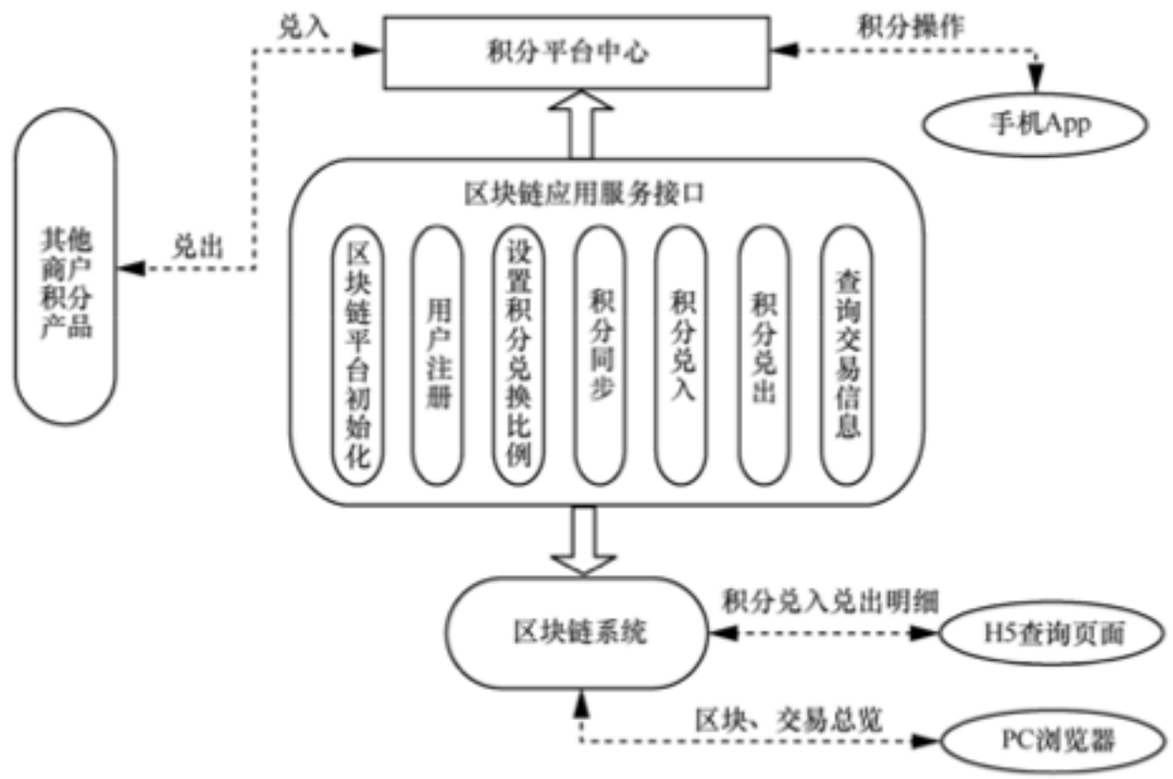
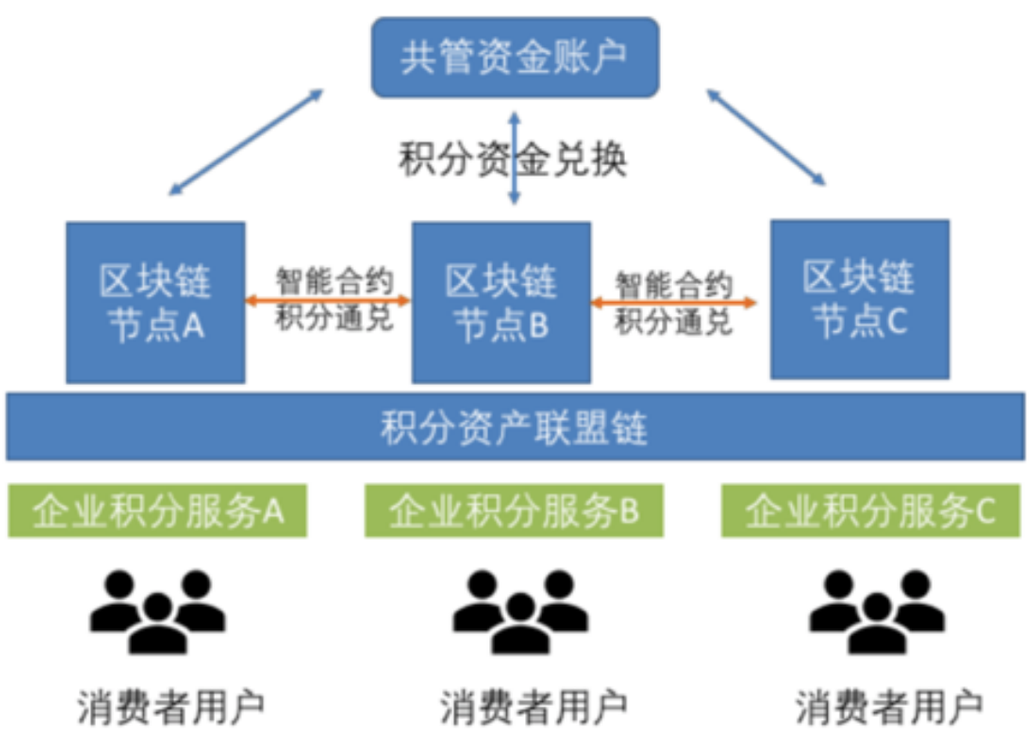
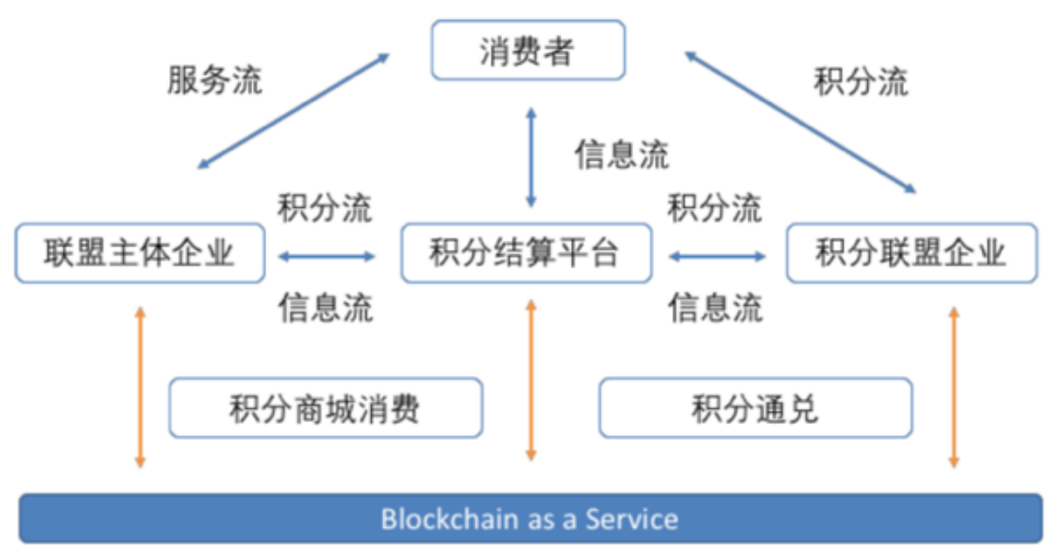


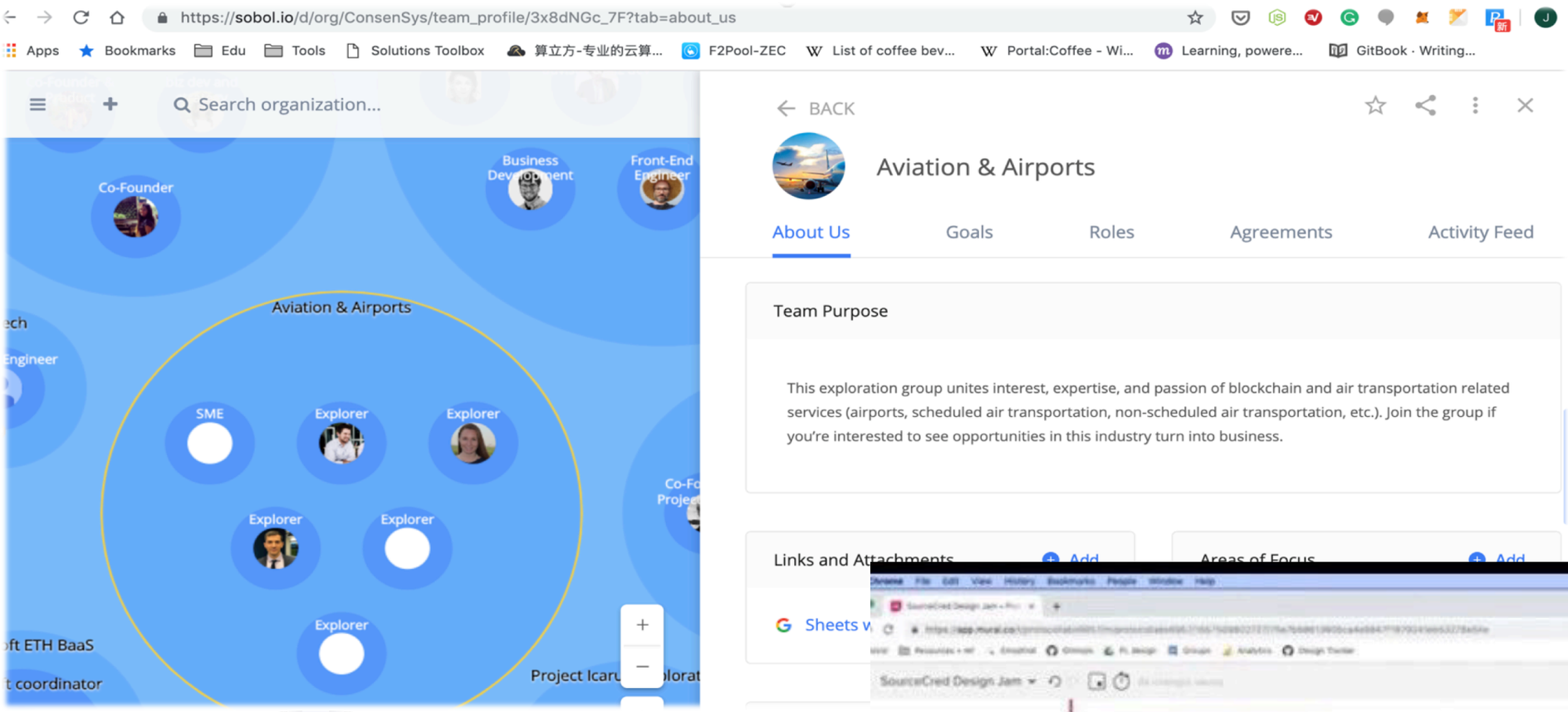
图 3　积分平台原型系统架构

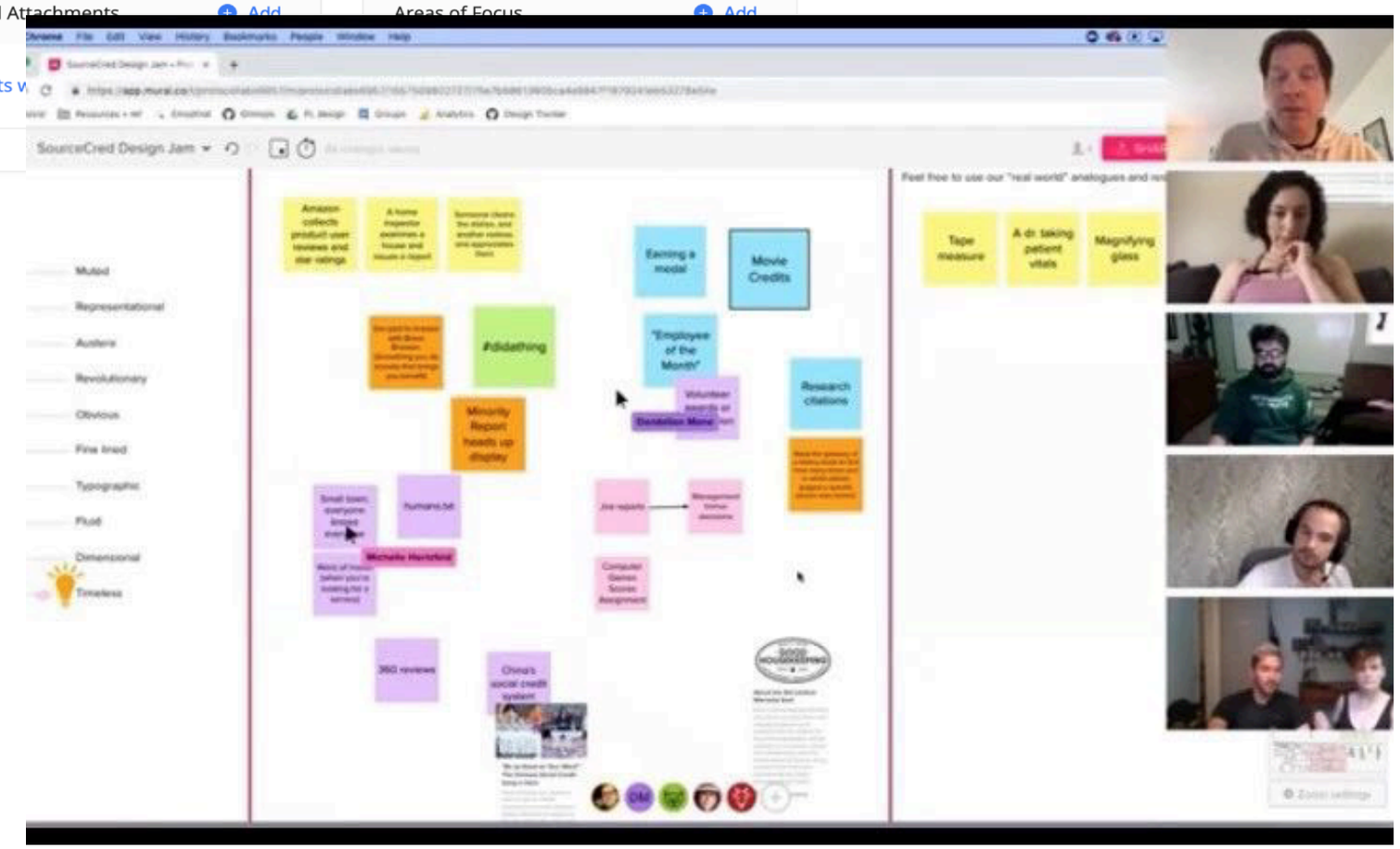




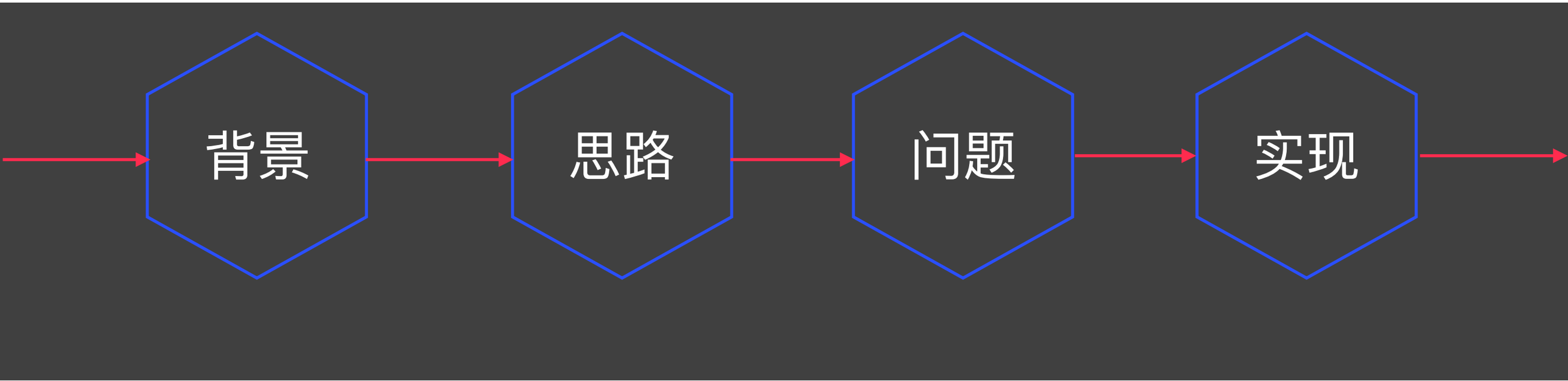
Blockchain Application

协同办公





课程项目例子
人脸验活

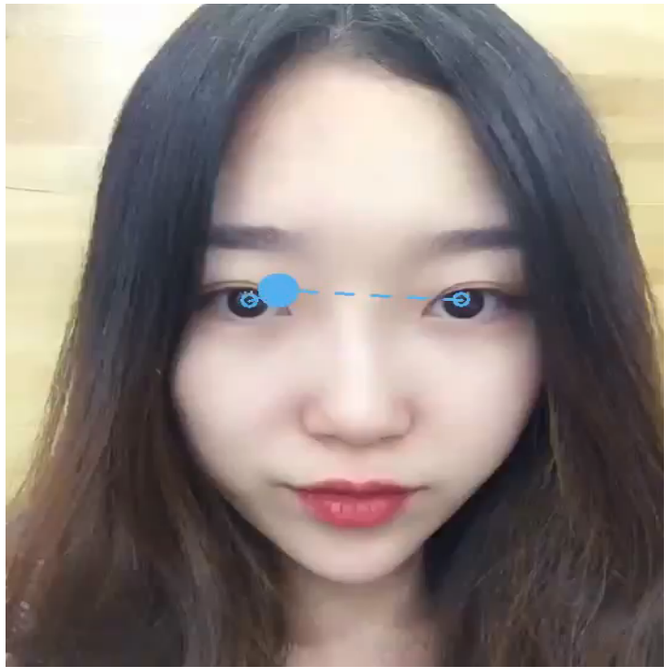


人脸验活

人脸识别技术中，验活环节具有关键意义。
针对人脸识别技术的攻击主要有以下类型：

1. **照片攻击**
2. **Video攻击**
3. **VR攻击**
4. **3D打印头套攻击**

其他：漏眼攻击



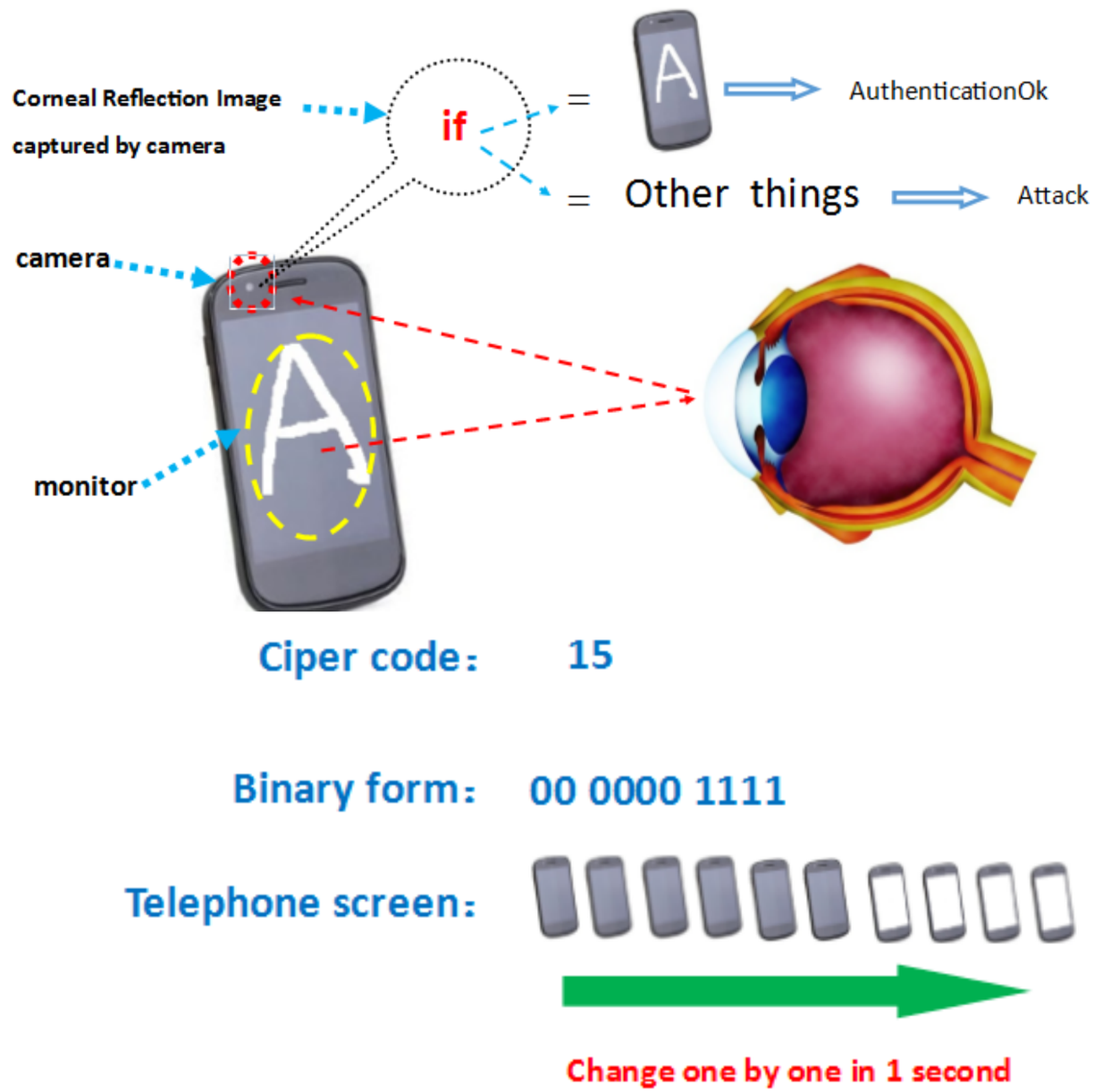
学术界的人脸验活研究现状：

1. **纹路质地分析验活（texture）**
2. **深度特征验活（景深）**
3. **实时响应（real-time response）**
4. **复合模型验活（multimodal）**
5. **凝视验活（gaze of eye）**
6. **角膜反射验活(corneal reflection)**
7. **人脸颜色水印验活（face reflection）**

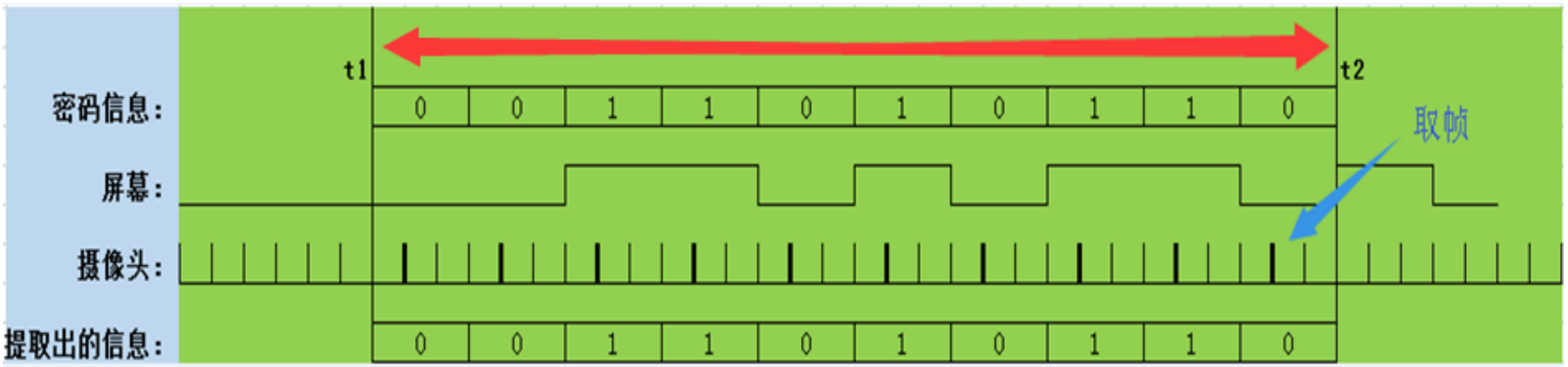
思想

方案思路:

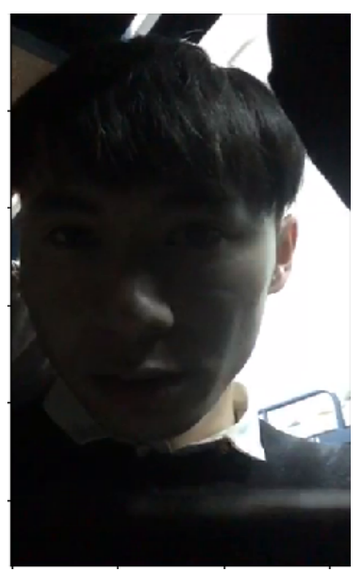
1. 用户使用手机进行人脸识别，摄像头正对着脸并保持约10cm的距离，眼睛保持睁开状态；
2. 手机随机生成一个0~1023之间的密码，并转换为二进制形式，通过屏幕亮暗的方式将密码发送出去。
3. 在屏幕发送密码信息之前，手机摄像头开启，并以视频录像的形式拍摄人脸信息。然后屏幕亮暗的变化，以此代表密码信息，并被角膜反射，为摄像头捕抓到。
4. 在屏幕发送完密码信息后，手机摄像头关闭录像，并把视频信息传输到后台处理程序。



问题

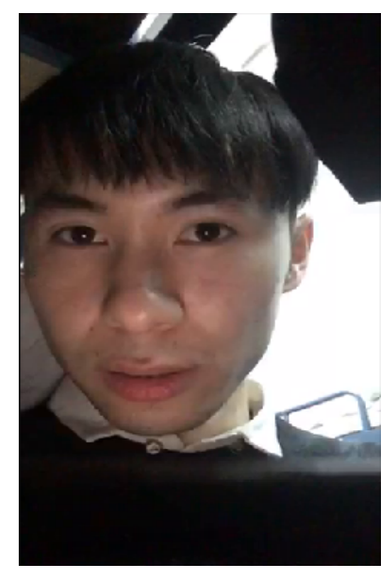


屏幕暗：
（0）

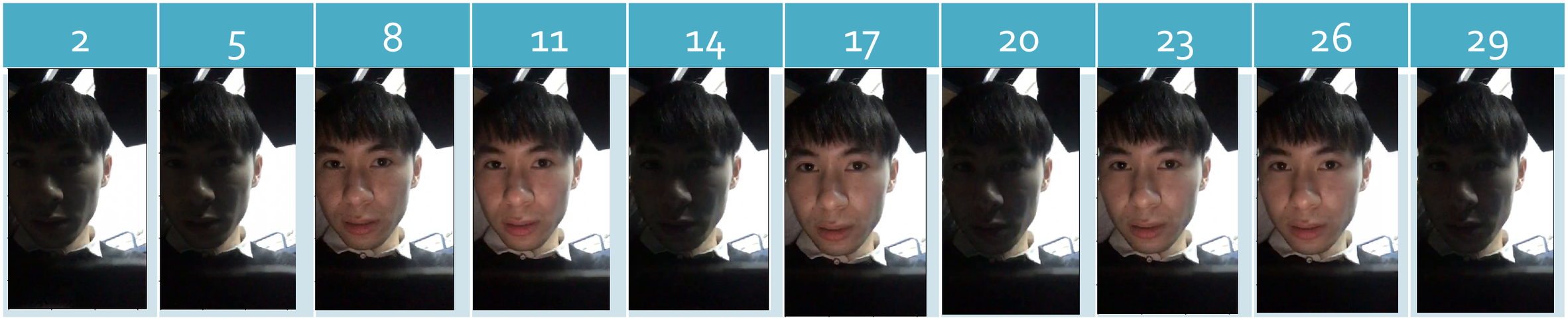


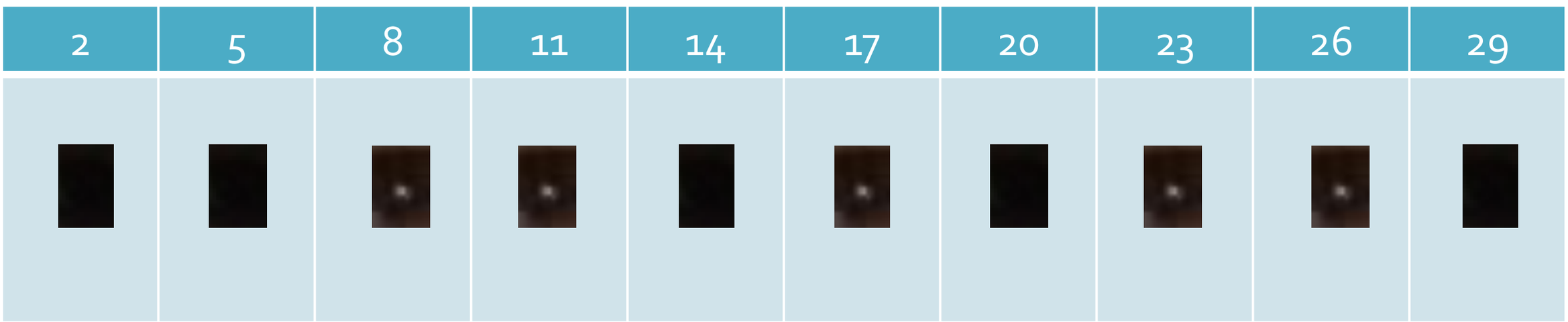
半帧：
（中间态）

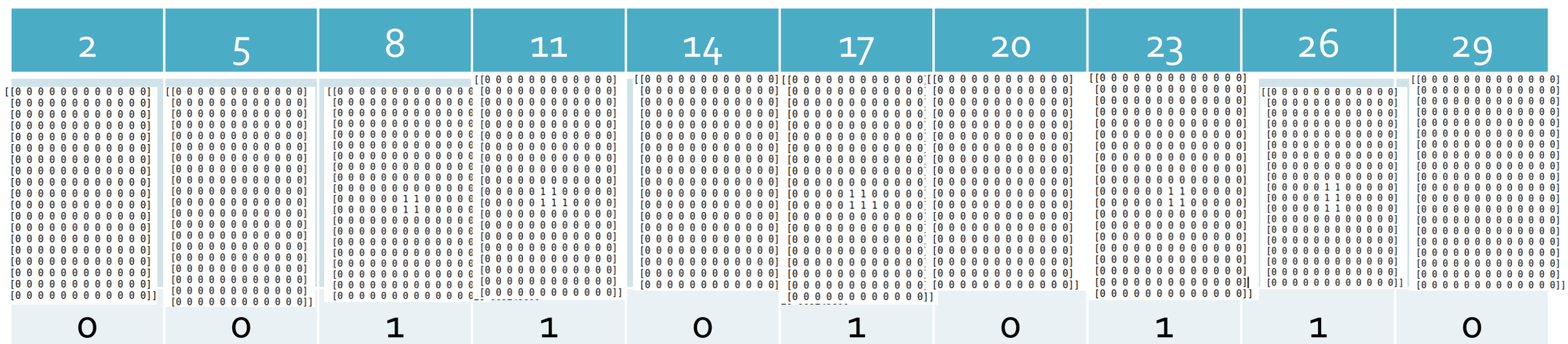
屏幕亮：
（1）



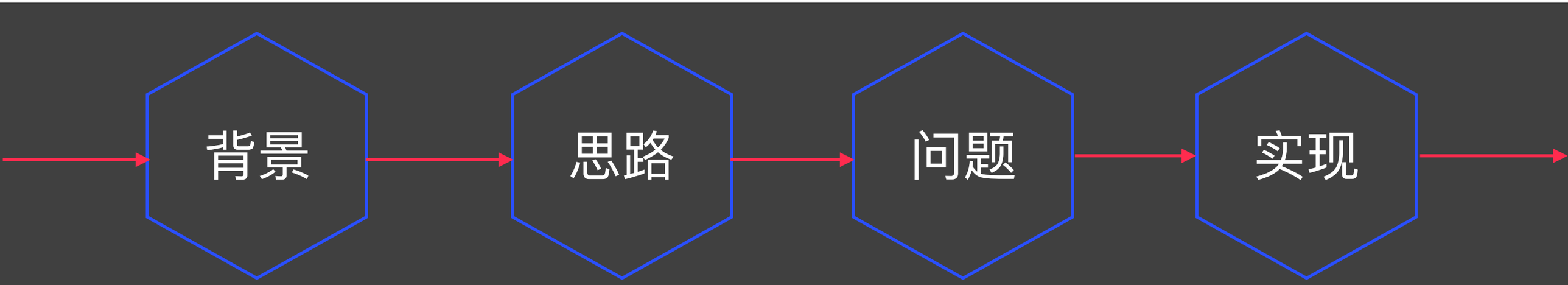
实现


2
5
8
11
14
17
20
23
26
29

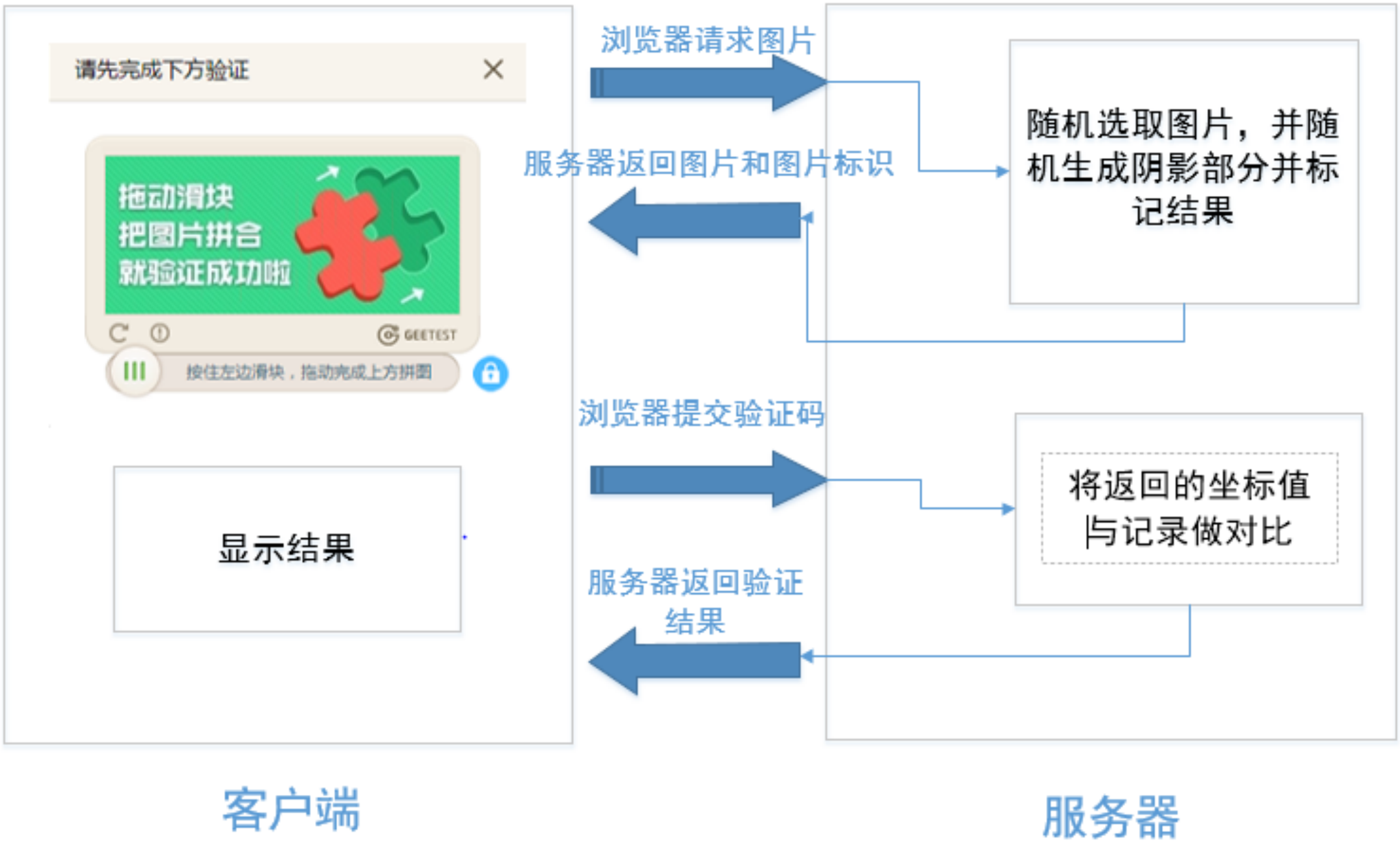

2
5
8
11
14
17
20
23
26
29


2
5
8
11
14
17
20
23
26
29
0
0
1
1
0
1
0
1
1
0

课程项目例子
滑动CAPTCHA



滑动CAPTCHA


请先完成下方验证
拖动滑块
把图片拼合
就验证成功啦
GEETEST
按住左边滑块，拖动完成上方拼图
显示结果
浏览器请求图片
服务器返回图片和图片标识
浏览器提交验证码
服务器返回验证结果
随机选取图片，并随机生成阴影部分并标记结果
将返回的坐标值与记录做对比
客户端
服务器

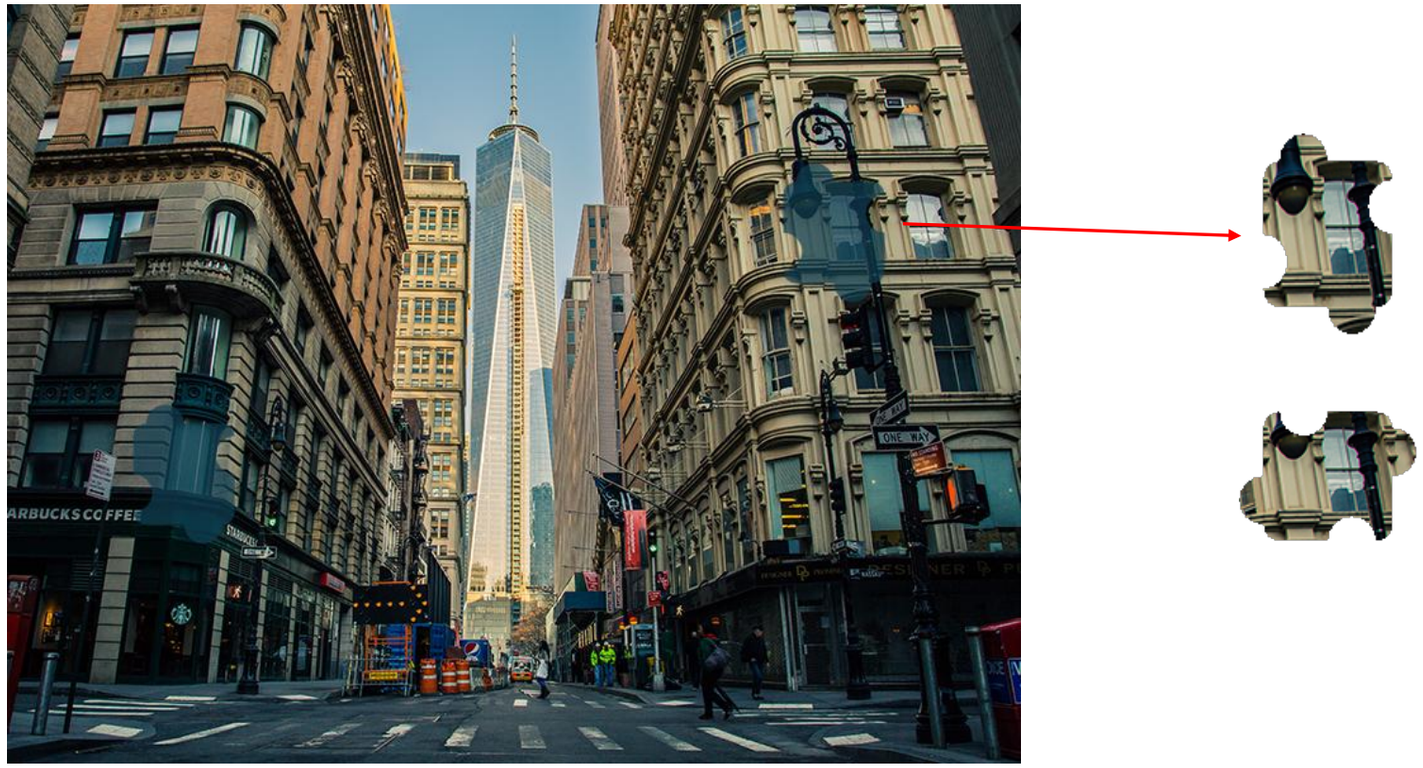
设计思路

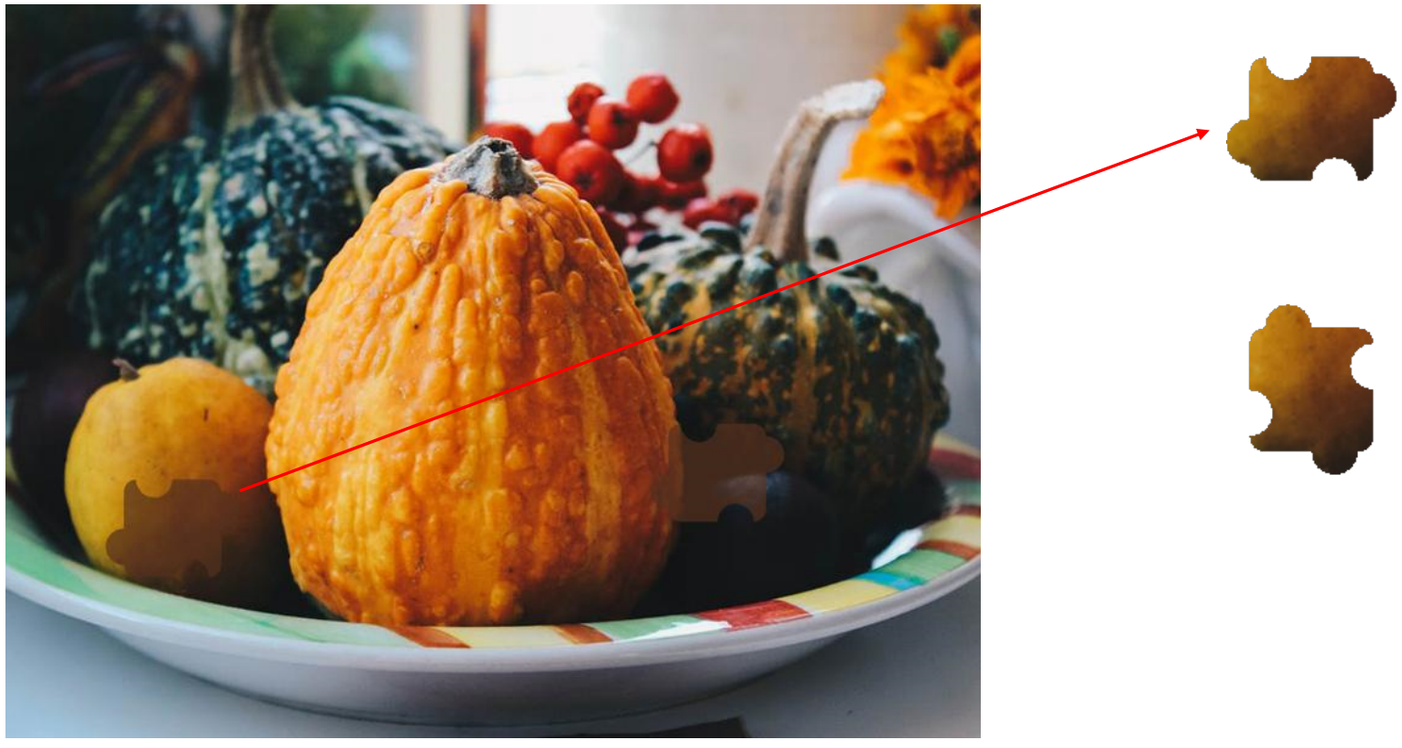
主要机制

真阴影区

假阴影区

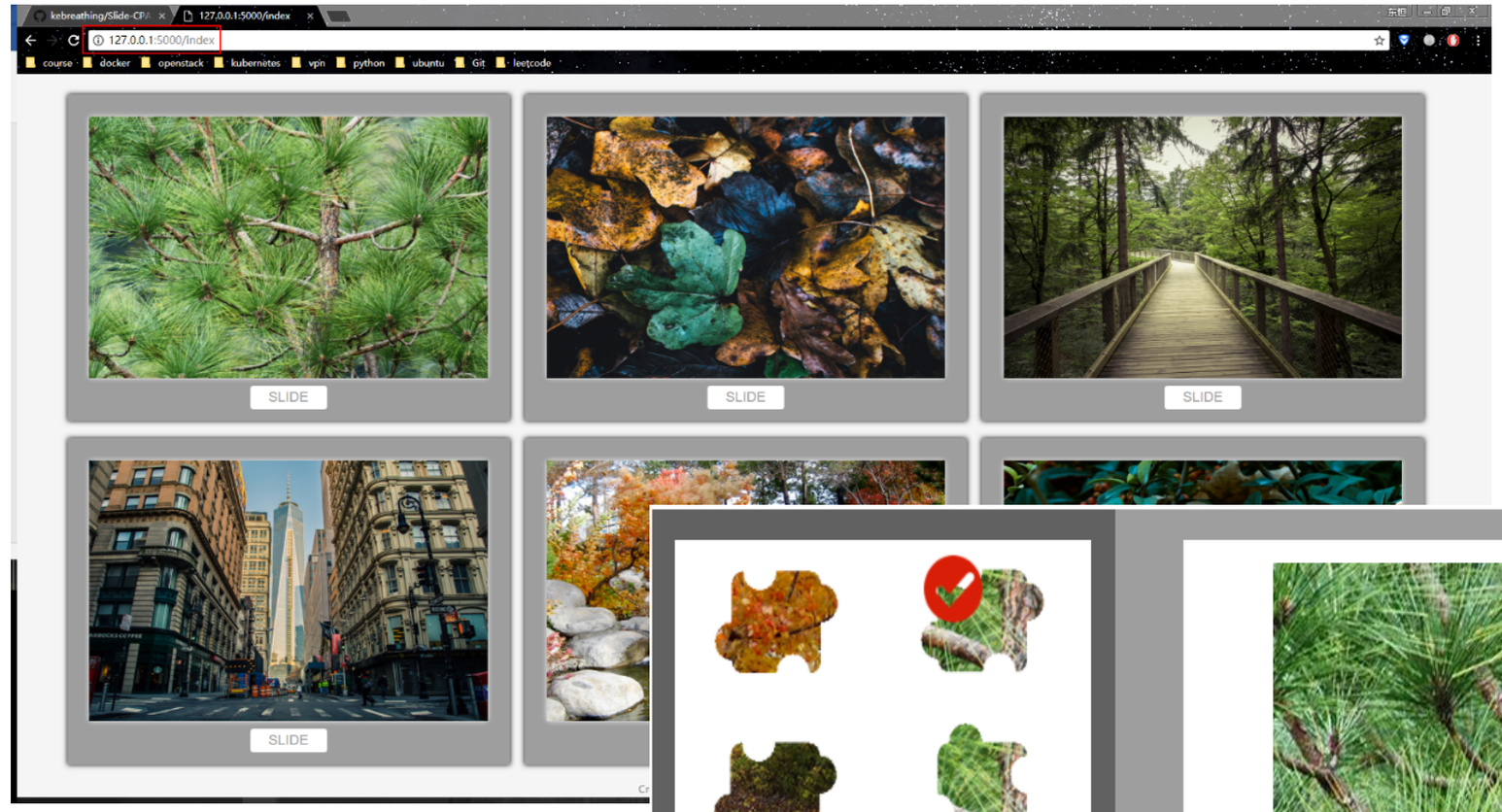
实现效果

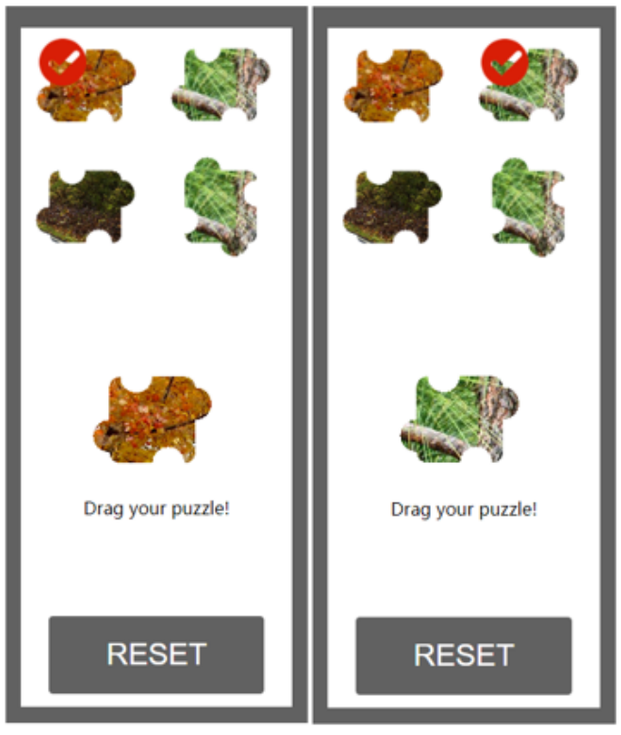


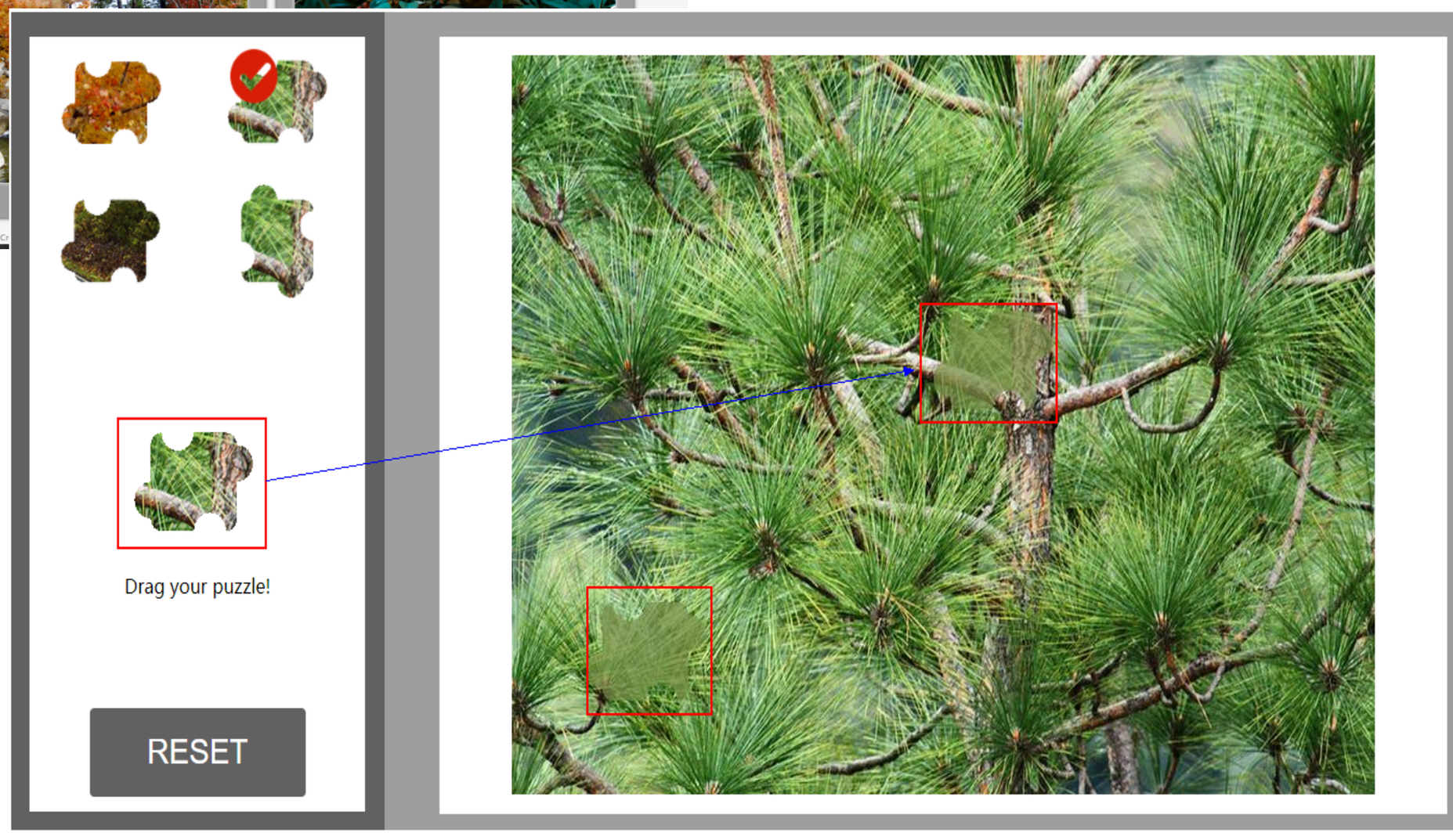


FaceLive

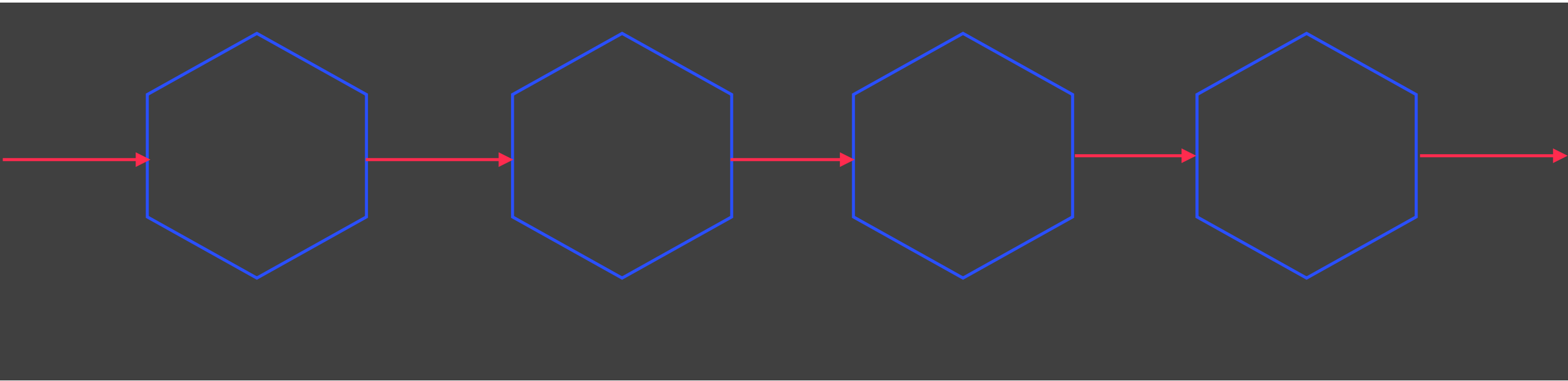
展示


127.0.0.1:5000/index
course
docker
openstack
kubernetes
vpn
python
ubuntu
Git
leetcode
SLIDE
SLIDE
SLIDE
SLIDE


Drag your puzzle!
RESET
Drag your puzzle!
RESET


Drag your puzzle!
RESET

课程项目交流



谢谢！

Huiping Sun
sunhp@ss.pku.edu.cn
https://huipingsun.github.io