区块链原理及保险业应用思考

- 本人以个人身份参加此次活动，所有言论与所在公司无关
- 本文中提到的以太坊、比特币等项目均为高风险项目，仅作技术分析，并非投资推荐

目录

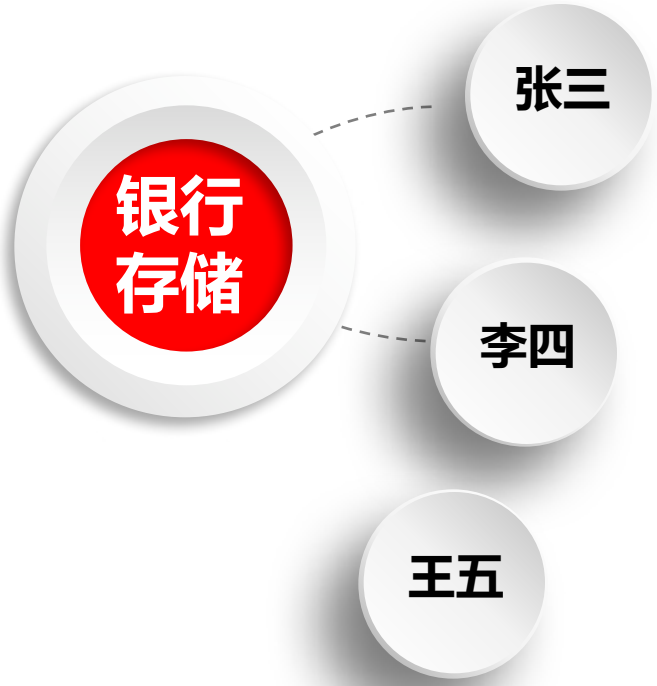
CATALOG

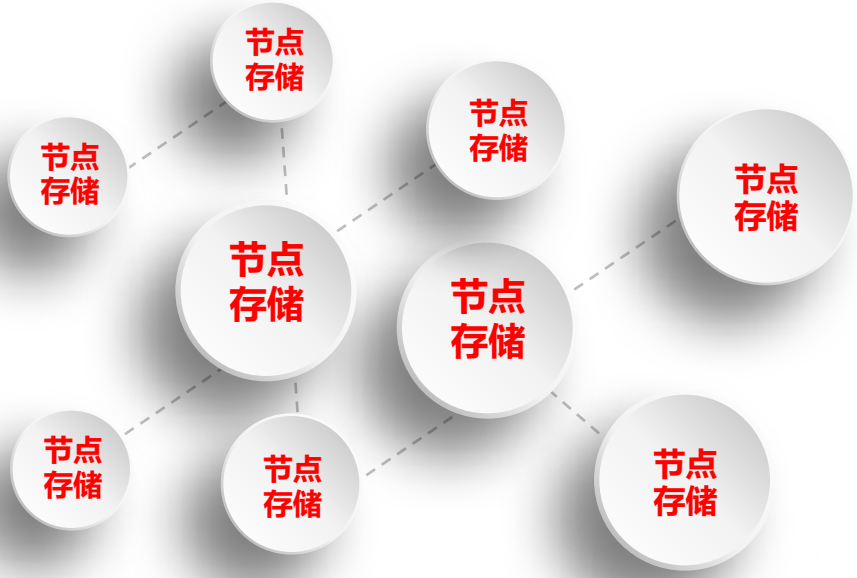
01

PART 01

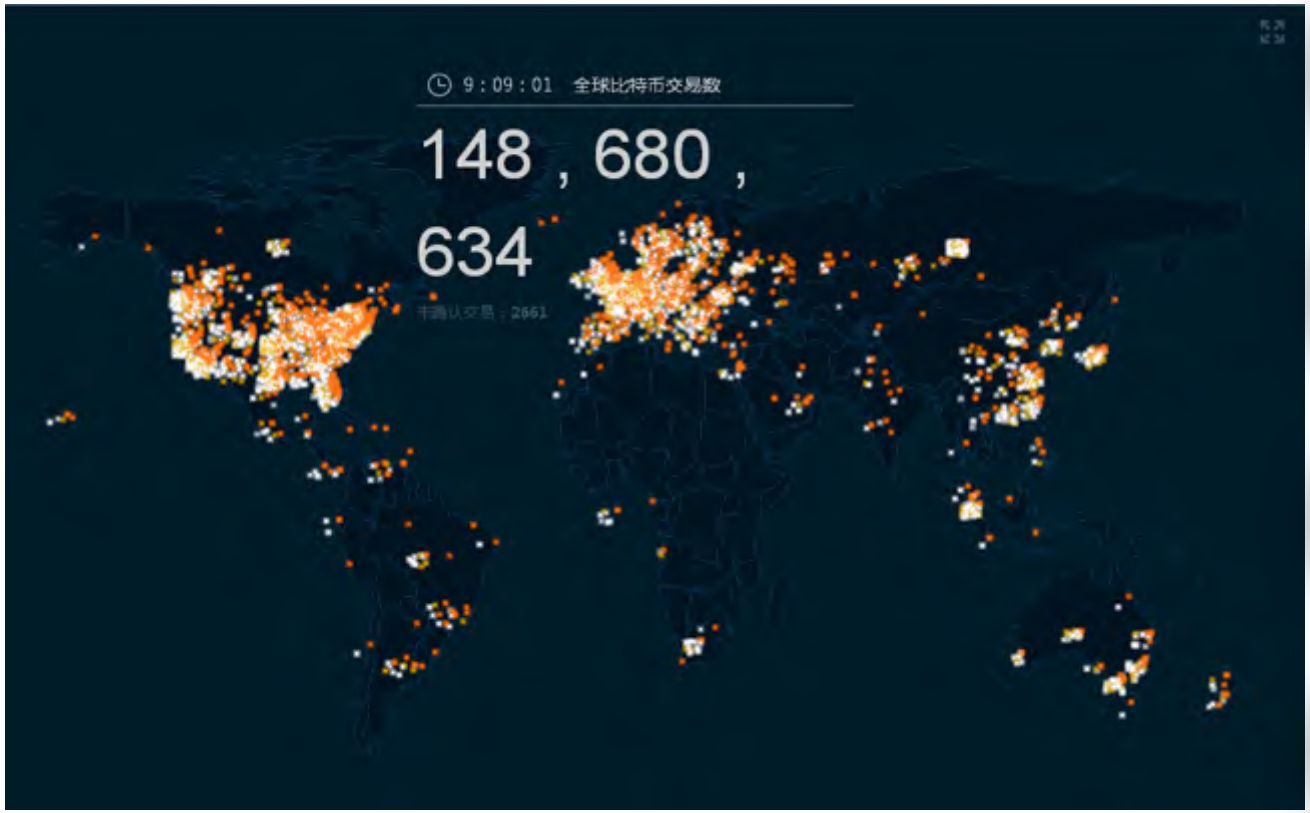
第一部分
区块链原理

只有银行服务器证明我有一元人民币，但全世界都证明我有一个比特币



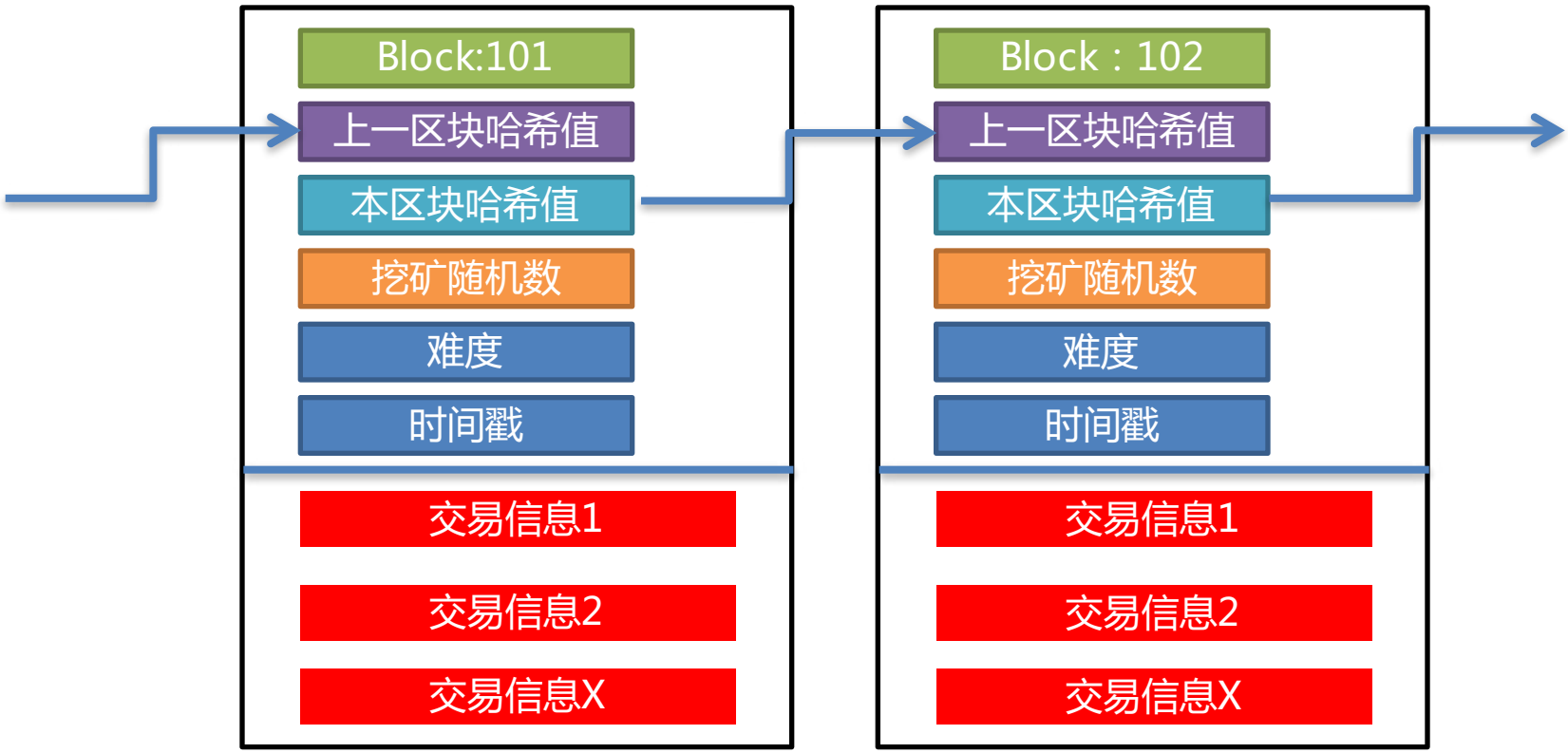


区块链想象成比特币网络的数据库

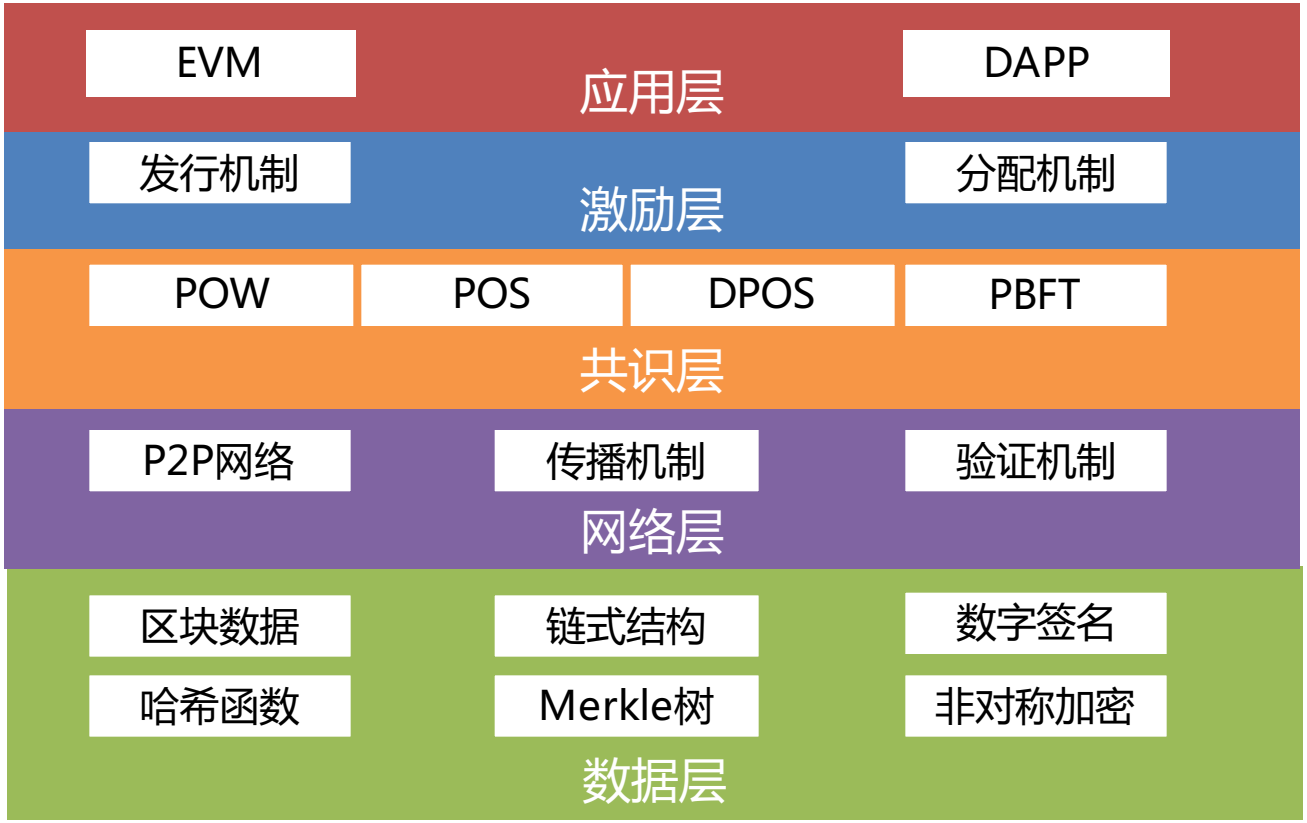


- 完整备份
- 历史记录
- 块状存储
- 交易广播

什么是区块和区块链


Block:101
上一区块哈希值
本区块哈希值
挖矿随机数
难度
时间戳
交易信息1
交易信息2
交易信息X
Block：102
上一区块哈希值
本区块哈希值
挖矿随机数
难度
时间戳
交易信息1
交易信息2
交易信息X

区块链基础架构


EVM
DAPP
应用层
发行机制
分配机制
激励层
POW
POS
DPOS
PBFT
共识层
P2P网络
传播机制
验证机制
网络层
区块数据
链式结构
数字签名
哈希函数
Merkle树
非对称加密
数据层

区块链如何实现去中心化

区块链通过非对称加密和数字签名对个人账户进行确权，通过全网所有节点数据比对来确认数据没有被篡改，但是

- 在点对点的网络中，如果部分节点故意篡改数据，影响其他节点怎么办？
- 如果作恶节点快速增加，怎么办？

区块链需要解决的第一个问题：拜占庭容错问题

区块链如何实现去中心化-拜占庭将军问题

刘备，关羽，张飞和魏延，任意两人都不是吕布的对手，所以必需三人联手才能打败吕布，所以进攻时必需三员将领同时上阵才能取胜，但是在将领中有叛徒，叛徒会假传命令，如何在这种情况下战胜吕布。

拜占庭问题实质就是分布式网络的一个最差错误模型，即错误节点可以做任意事情，比如不响应、发送错误信息、节点篡改数据甚至联合作恶等，总之，没有节点会出现比拜占庭将军问题更严重的错误。在这种情况下，分布式系统领域如何保证系统的一致性。

工作量证明（Proof of Work, POW）--挖矿

所有节点都平等的计算一个数学难题，最先获得答案的节点将获得这个区块的发布权。全网算力同时形成区块链的一道防火墙，降低黑客攻击风险。

SHA256(SHA256(Version+HashPreBlock + Merkle_root + Timestamp + Bits + Nonce)) ≤ 难度数

- 难度数：目标哈希值，根据全网算力动态变化
- Nonce：矿工不断尝试的随机数，小于TargetHash的Nonce就是答案。
- Merkle Tree：一种哈希二叉树,使用它可以快速校验大规模数据的完整性。

工作量证明如何解决节点作恶

一 让作恶增加成本

二 让大量增加作恶节点没有意义

三 让作恶收益不如做好事收益高

工作量证明带来的新攻击方法

- 51%攻击

  51%攻击并不能修改数据，但是可以产生“双花”攻击

1. 利用算力在另一条链偷偷挖矿而不广播
2. 在主链上将比特币卖出换取美元，此时主链增长了9个块，供给链10个块
3. 得到美元后立刻将攻击链公开广播
4. 主链被更长的攻击链取代，黑客账户的比特币转账被取消

其他共识算法

PBFT	股权证明 POS	授权股权 DPOS
• 通过数学算法实现,不需代币，33%容错，适合联盟链	• 股份制，通过币天数决定记账权，适合公有链	• 民主议会制，通过选举决定记账权，适合公有链

区块链如何实现去中心化

- 在点对点的网络中，数字资产属于纯粹的信息，可以轻易的复制，如何防止恶意节点多次消费？

区块链需要解决的第二个问题：双花问题

区块链如何实现去中心化

“双花”问题的解决办法：

全网广播所有交易并同步所有账户的状态

由此带来隐私的问题，目前有三个解决方法

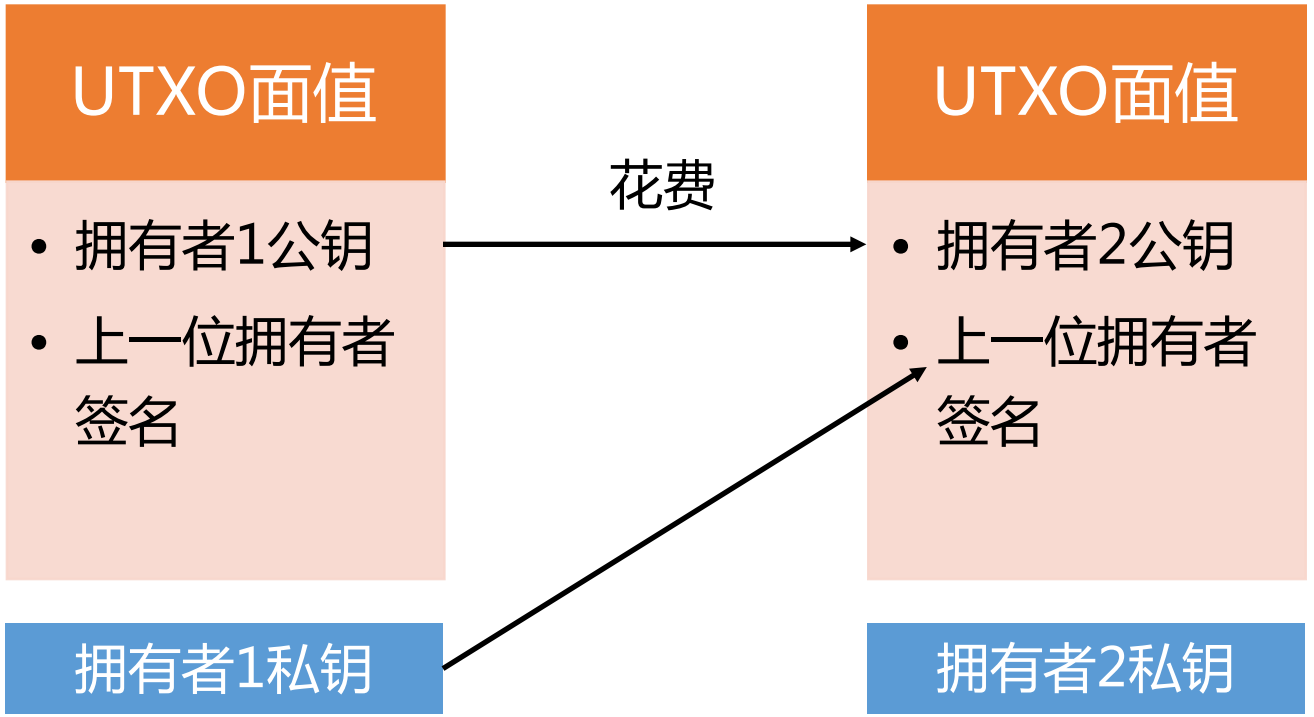
区块链如何实现去中心化

- 在点对点的网络中，交易是依赖数字签名来确保是由拥有者发出的，但如果攻击者获取了一笔合法的交易数据，然后再次广播出去，造成该笔交易再次执行怎么办？

区块链需要解决的第三个问题：重放攻击

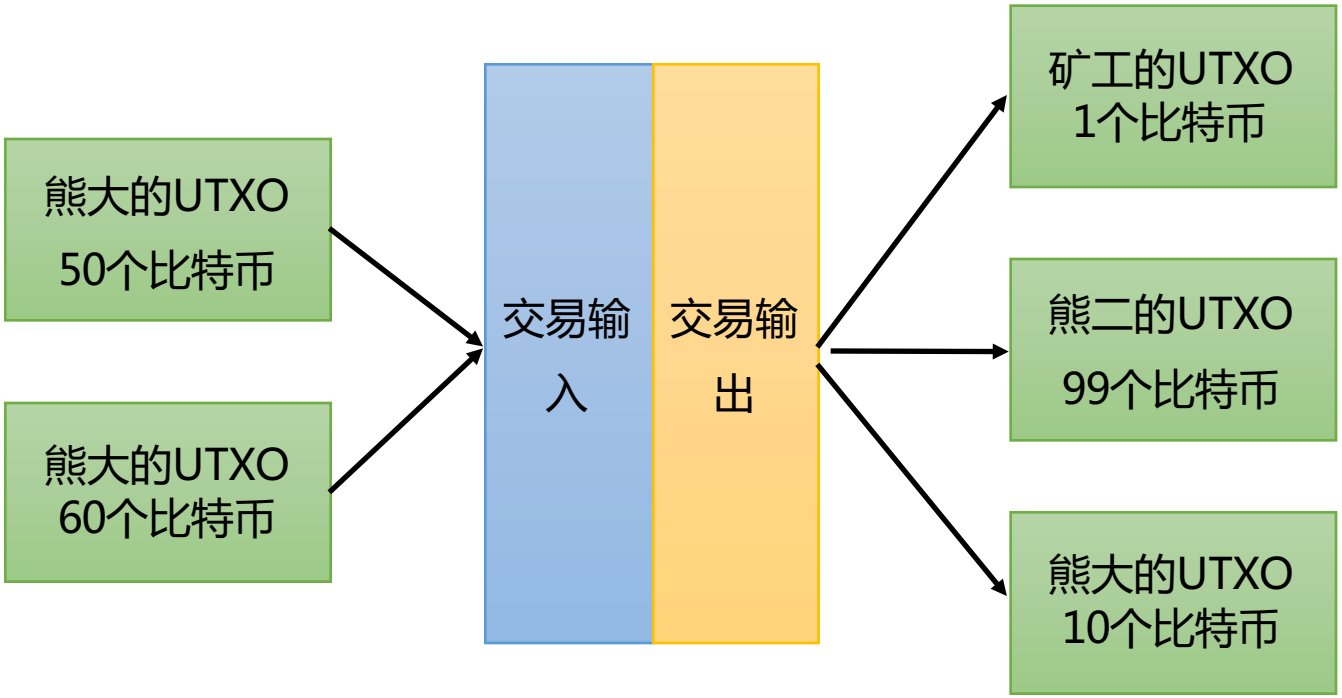
区块链如何实现去中心化

UTXO（未花费的交易输出）



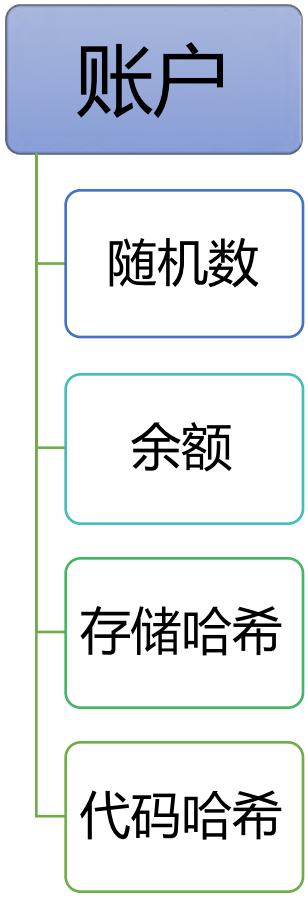
区块链如何实现去中心化

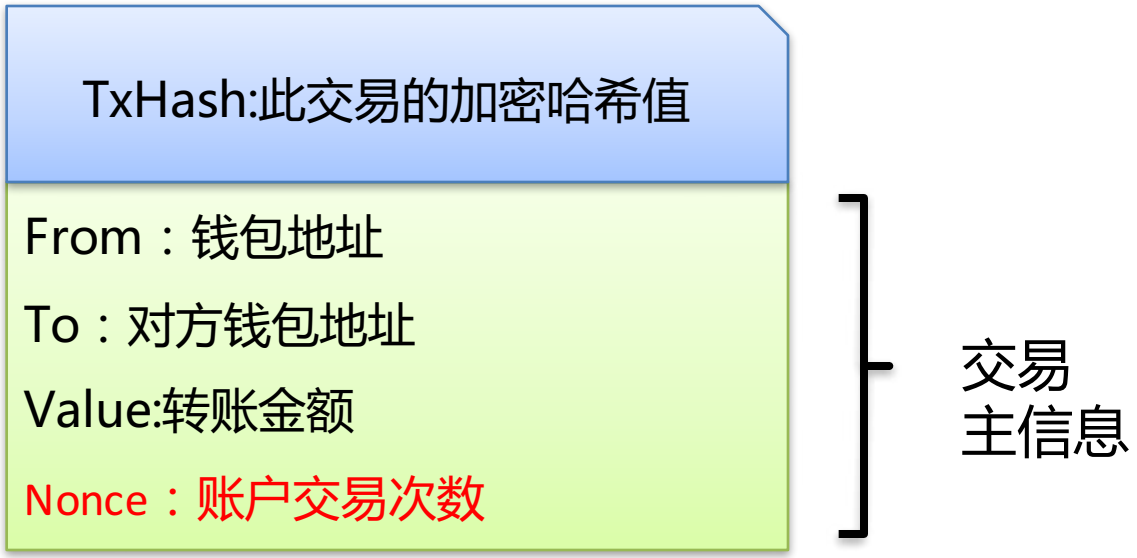
UTXO（未花费的交易输出）



区块链如何实现去中心化

账户模式





02

PART 02

第二部分
智能合约

※ 区块与链

※ 特征分类

※ 技术架构

※ 演化史

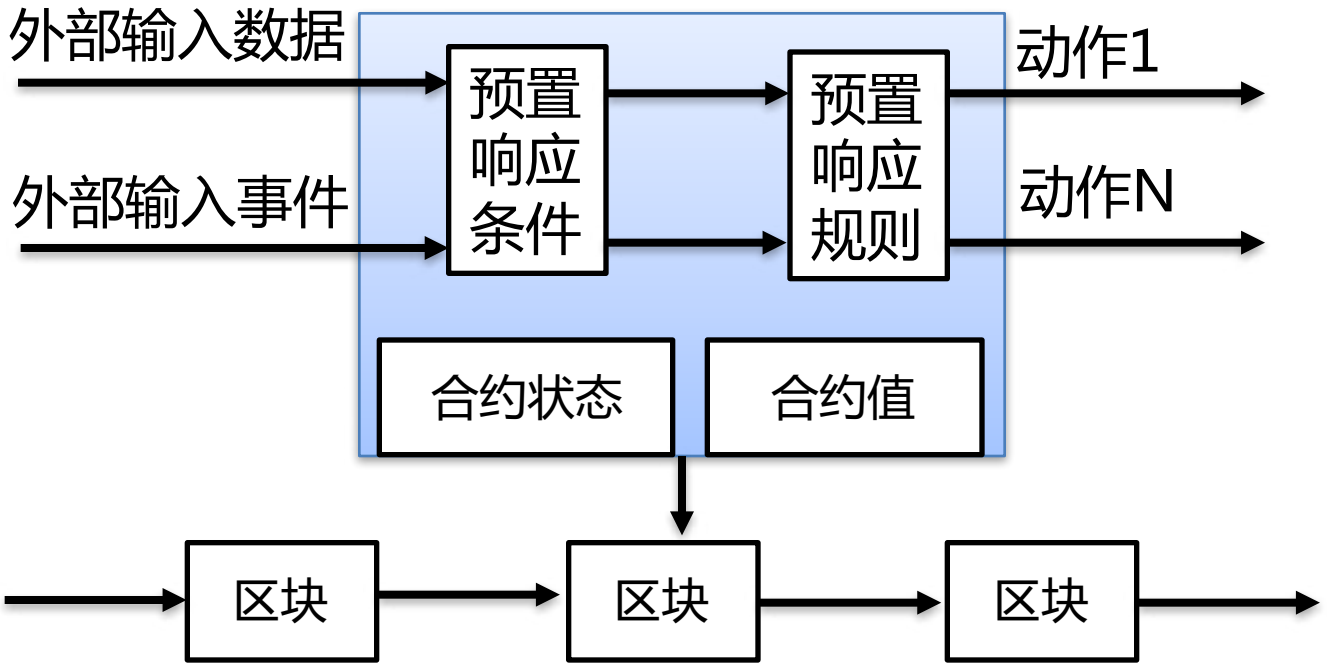
什么是智能合约？

（目前尚没有明确定义）

智能合约是由事件驱动的、具有状态的、获得多方承认的、运行在一个可信、共享的区块链账本之上的、且能够根据预设条件自动处理账本上资产的程序。

智能合约的优势是利用程序算法替代人仲裁和执行资产。

智能合约模型



智能合约长什么样？

```
contract Sample
{       uint value; //定义变量
        function Sample(uint v) {  //初始化
        value = v;       }
        function set(uint v) { //定义存储函数
                value = v;       }
        //定义取值函数
        function get() constant returns (uint) {
                return value;
        }
}
```

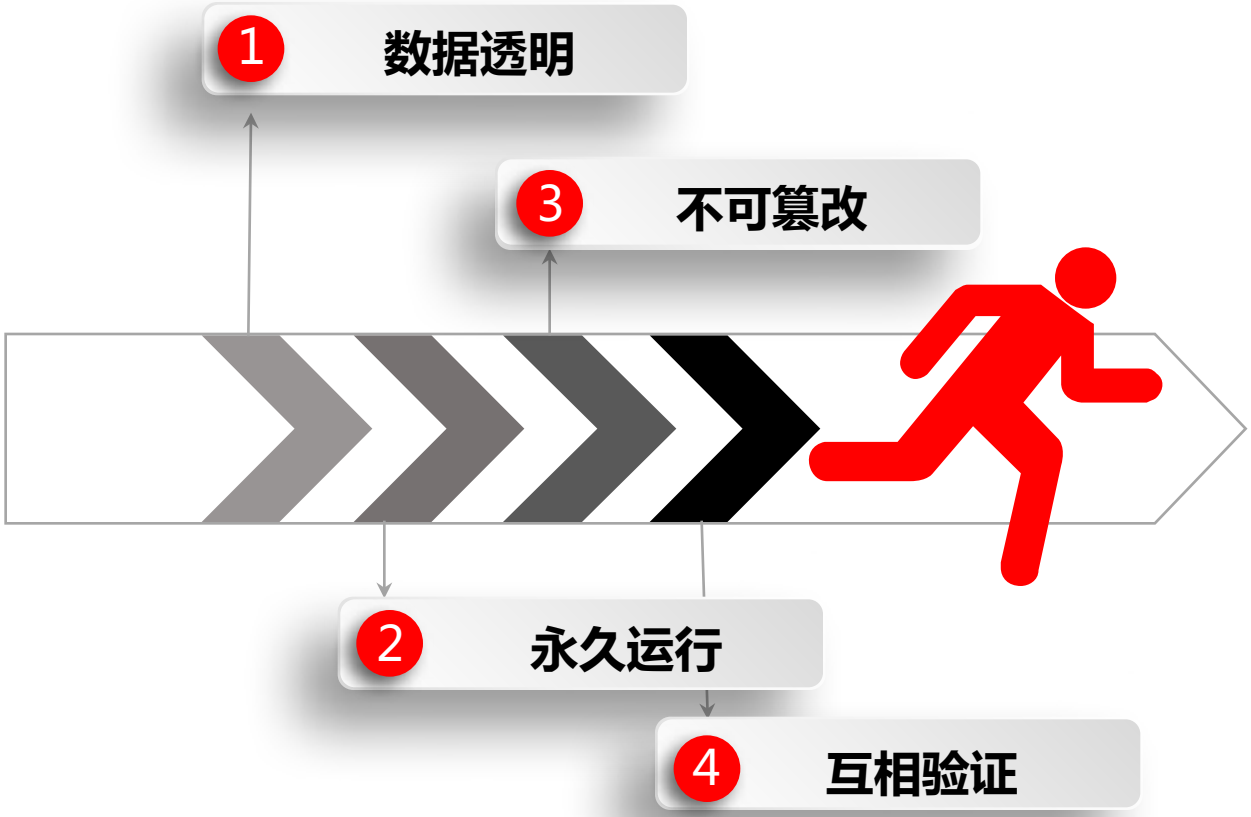
Solidity

Go语言

JAVA

自定义语言

为什么传统IT系统不能叫智能合约？



以太坊虚拟机（EVM）

以太坊中智能合约的运行环境。如果做比喻的话智能合约运行更像是JAVA程序，JAVA程序通过JAVA虚拟机（JVM）将代码解释字节进行执行，以太坊的智能合约通过以太坊虚拟机（EVM）解释成字节码进行执行。

交易数据中加入了Input data

TxHash:此交易的加密哈希值

From：钱包地址

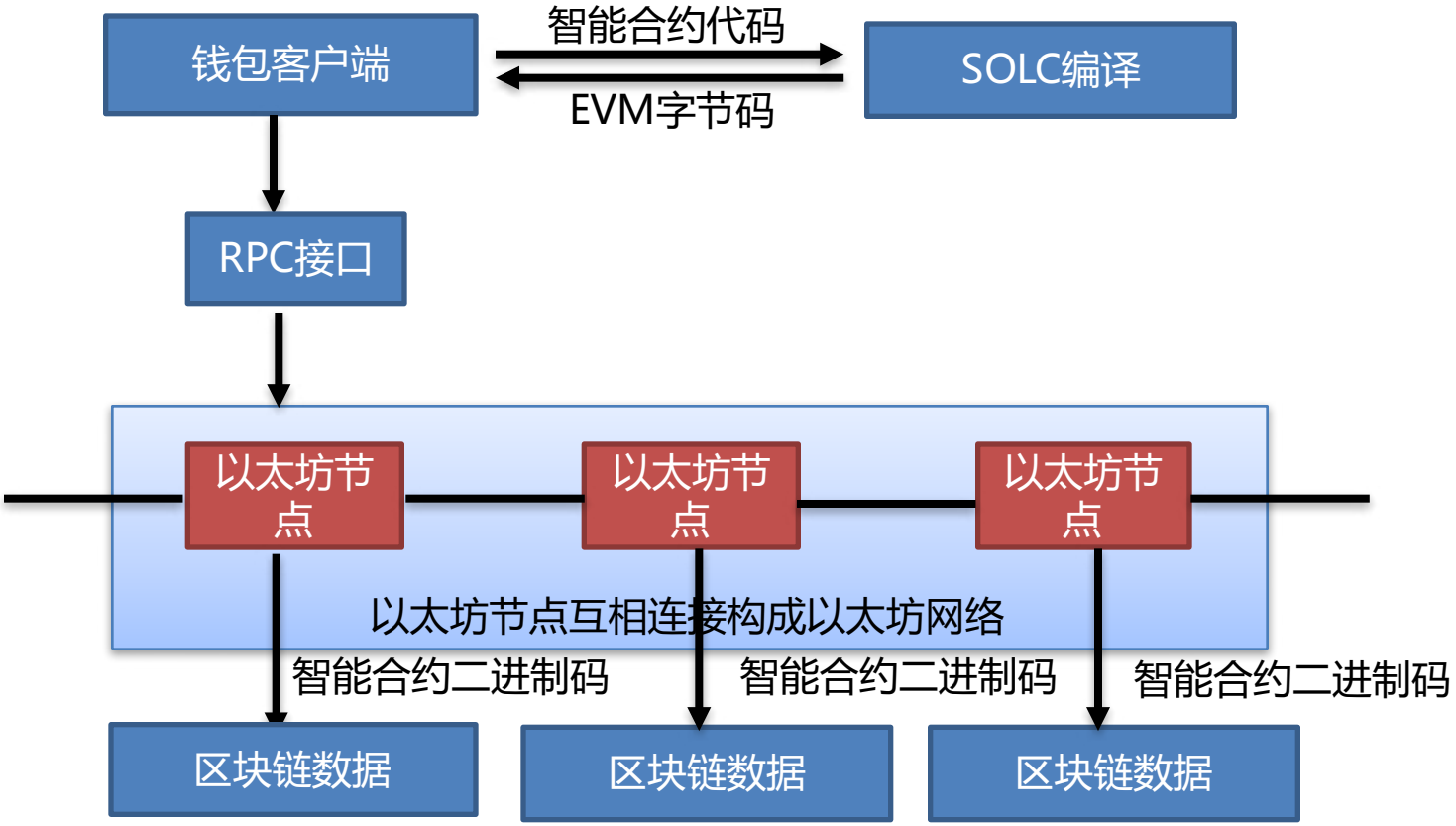
To：对方钱包地址

Value:转账金额

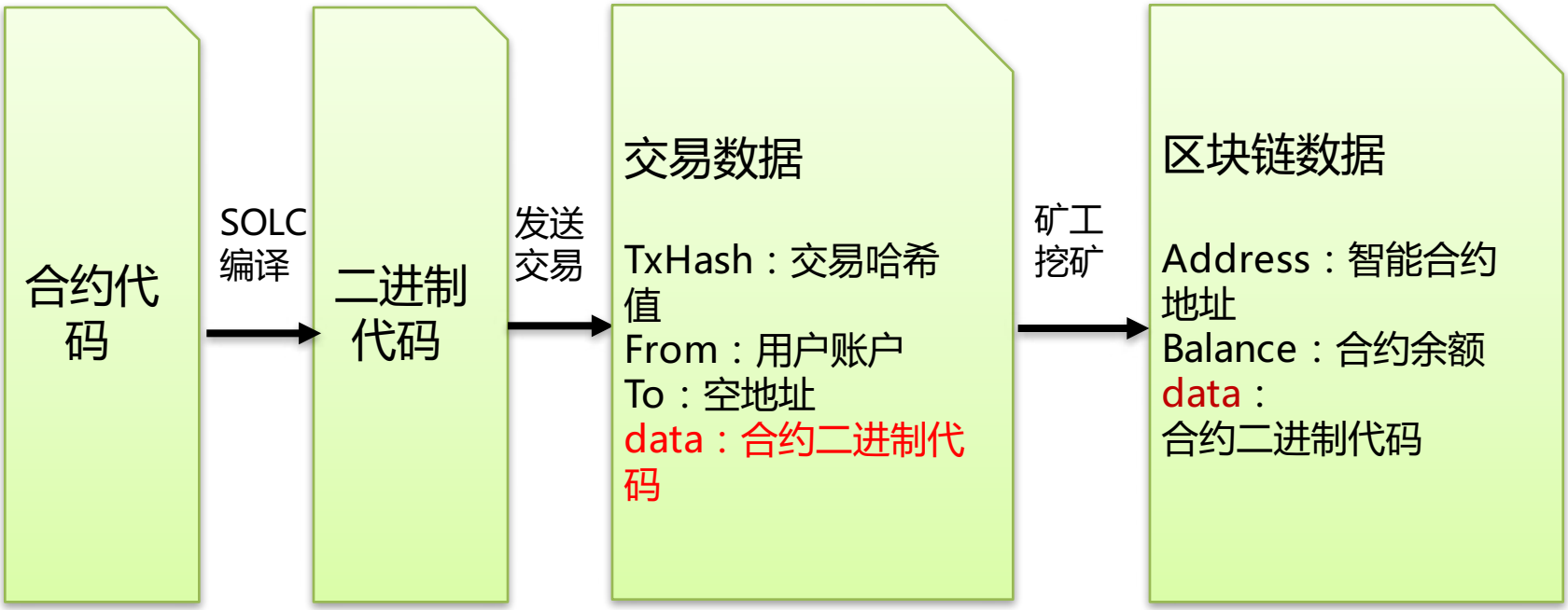
Input data：输入的数据、变量

交易主信息

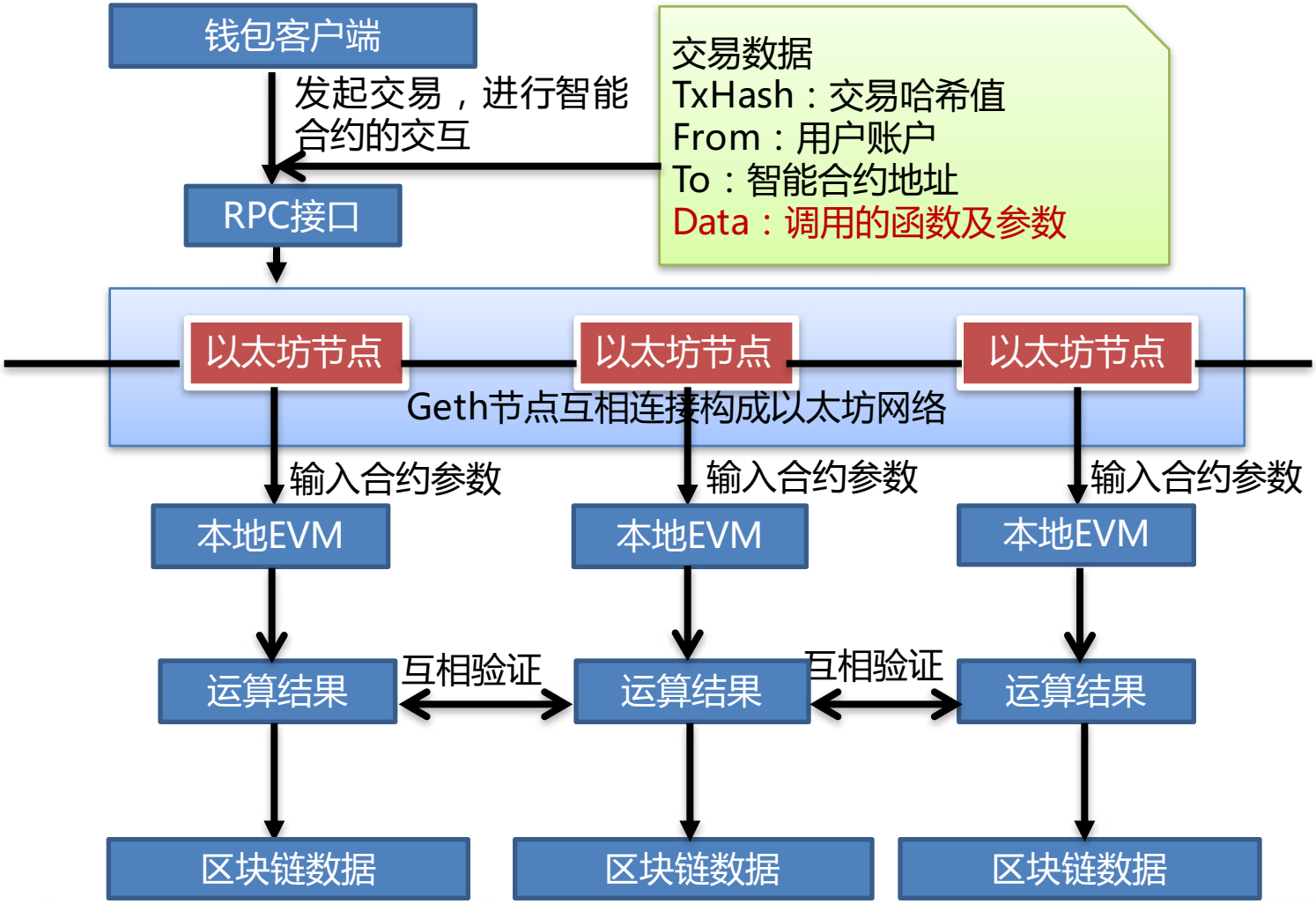
智能合约部署原理


钱包客户端
智能合约代码
EVM字节码
SOLC编译
RPC接口
以太坊节点
以太坊节点
以太坊节点
以太坊节点互相连接构成以太坊网络
智能合约二进制码
智能合约二进制码
智能合约二进制码
区块链数据
区块链数据
区块链数据

部署的数据流


合约代码
SOLC编译
二进制代码
发送交易
交易数据
TxHash：交易哈希值
From：用户账户
To：空地址
data：合约二进制代码
矿工挖矿
区块链数据
Address：智能合约地址
Balance：合约余额
data：
合约二进制代码

智能合约运行原理


钱包客户端
发起交易，进行智能合约的交互
交易数据
TxHash：交易哈希值
From：用户账户
To：智能合约地址
Data：调用的函数及参数
RPC接口
以太坊节点
以太坊节点
以太坊节点
Geth节点互相连接构成以太坊网络
输入合约参数
输入合约参数
输入合约参数
本地EVM
本地EVM
本地EVM
运算结果
互相验证
运算结果
互相验证
运算结果
区块链数据
区块链数据
区块链数据

智能合约面临的问题

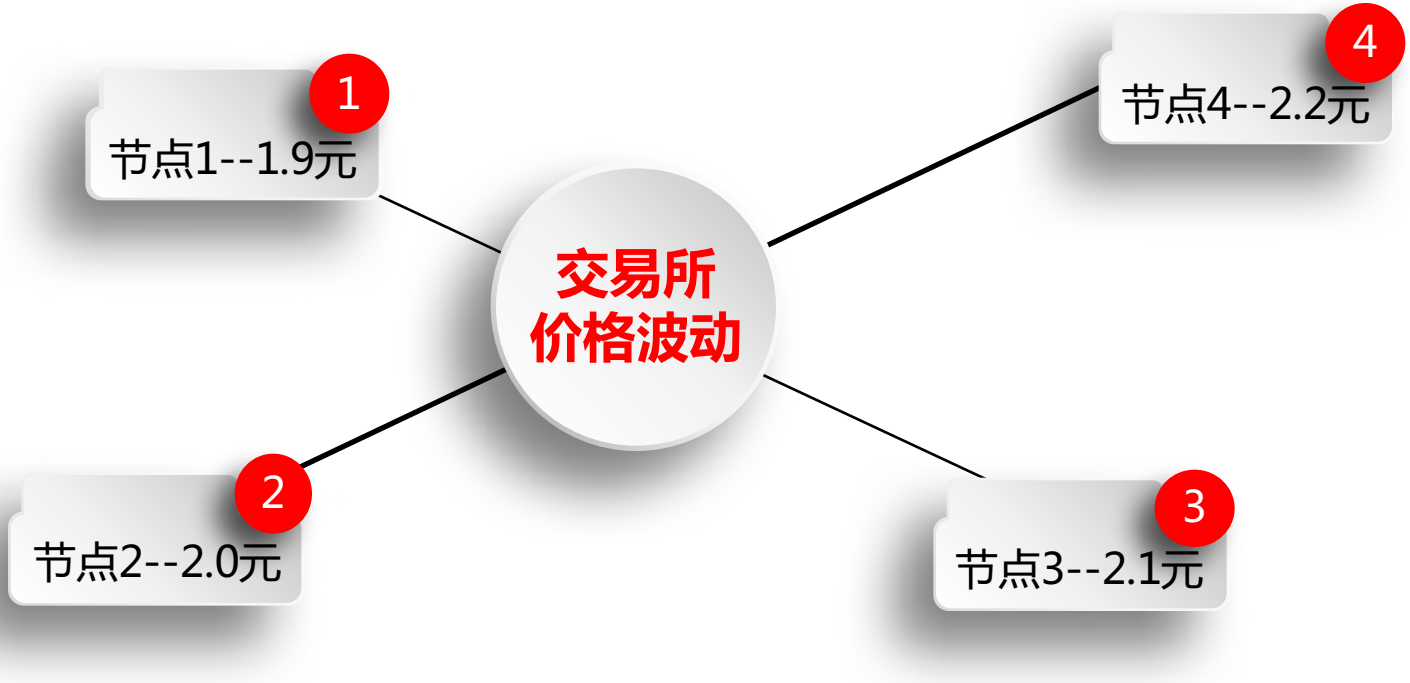
- 如果有人提交1T代码量的智能合约给区块链怎么办？
- 如果智能合约出现无限循环代码怎么办？

智能合约示例及GAS消耗

```
1  //Sample contract
2  contract Sample
3  {
4      uint value;
5      function Sample(uint v) { max execution cost: 20147 gas
6          value = v;
7      }
8      function set(uint v) { max execution cost: 20138 gas
9          value = v;
10     }
11     function get() constant returns (uint) { max execution cost: 247 gas
12         return value;
13     }
14 }
15
```

以上代码部署并运行一次，约合人民币0.1元

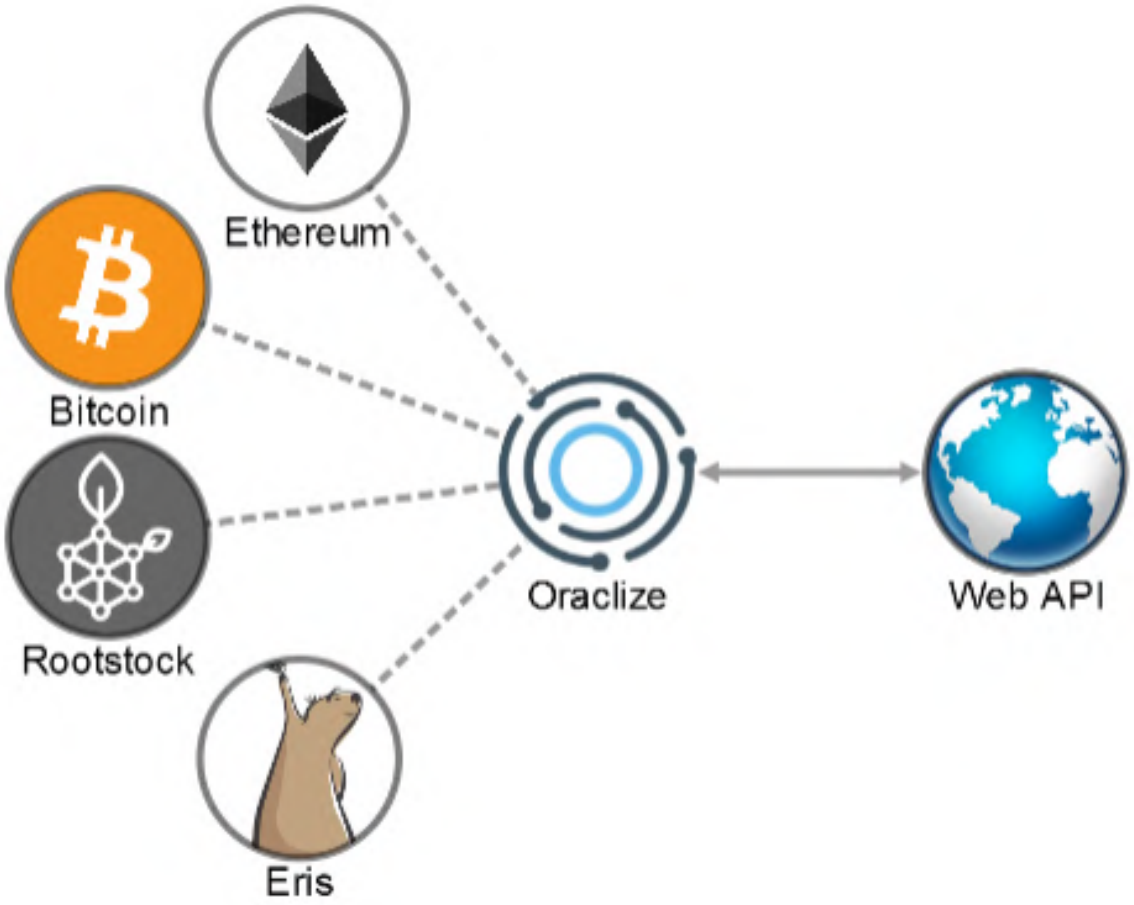
智能合约如何可信的与外部世界交互



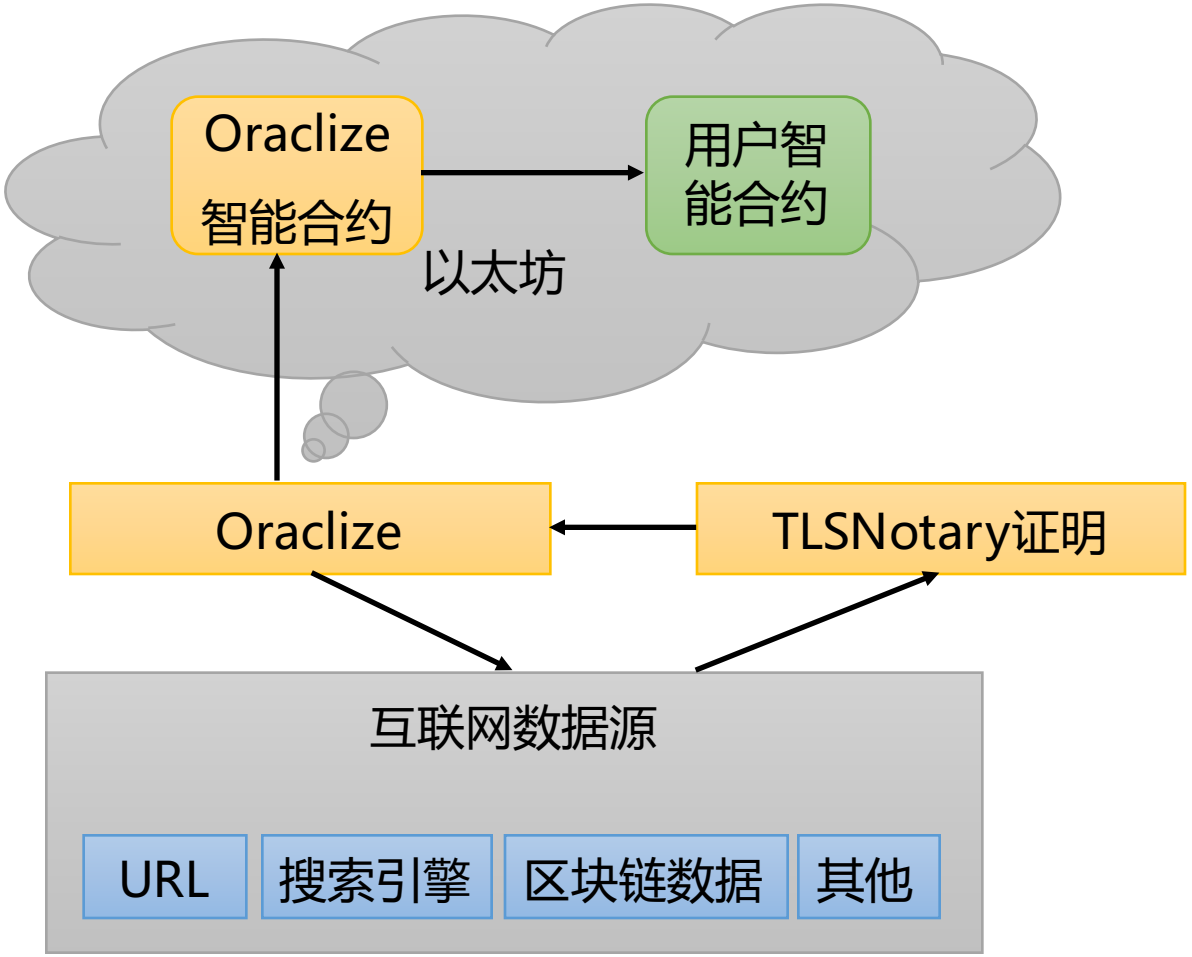
1、主动获取价格时，各节点获取价格不一致怎么办？

2、被动输送价格时，如何信任提供数据的第三方

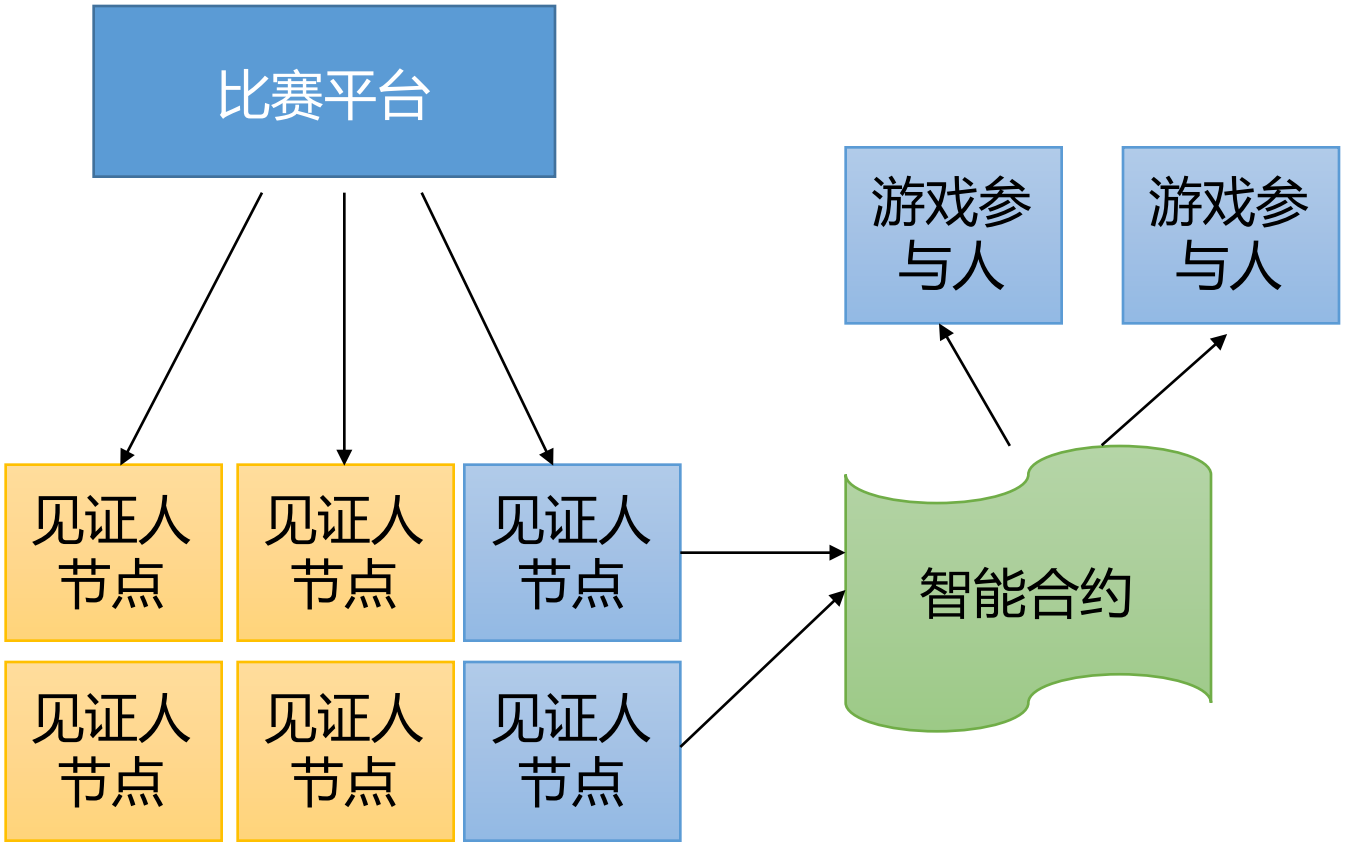
通过单个Oracle获取



通过单个Oracle获取



通过多重Oracle获取



03

PART 03

第三部分
区块链应用

※ 比特币本质　　※ 相互保险

※ 个人征信　　※ 农业保险

比特币能否作为货币应用于经济？

螺旋式通缩最后导致经济逐步停滞

银行业实现的电子现金的特性

- 独立性：密码学安全
- 不可重复花费
- 匿名性
- 不可伪造性
- 可传递性
- 可分性

那么比特币是什么？

Bitcoin：A Peer-to-Peer Electronic Cash System

基础货币 currency

1. 法定准备金
2. 超额准备金
3. 公众现金
4. 银行库存现金

现金流通方式

1. 纸钞
2. 银行IC卡
3. 比特币
4. Modex等电子现金系统

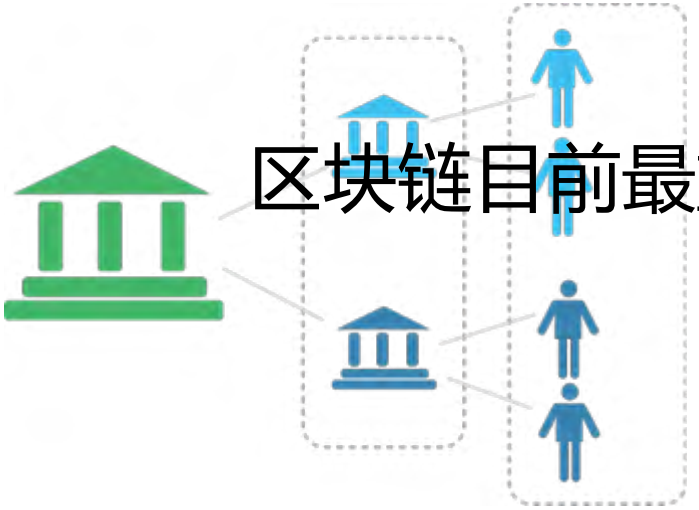
区块链应用注意事项

1. 区块链和智能合约能实现的，现在有IT系统都能实现，区块链是去掉中介
2. 区块链实现的不是性能的提升，而是业务模式的改变，相反性能大幅度下降，核心是去中介化
3. 只能实现对链内内生的信息信任，对外界引入的信息无法建立信任
4. 区块链应用不需要币

区块链伪应用 ：1、智能合约实现保险自动理赔 2、区块链实现海淘奶粉防伪

最重要的应用领域是金融业和各行业金融属性部分

区块链目前最重要的应用升职加薪



传统金融模式

区块链模式

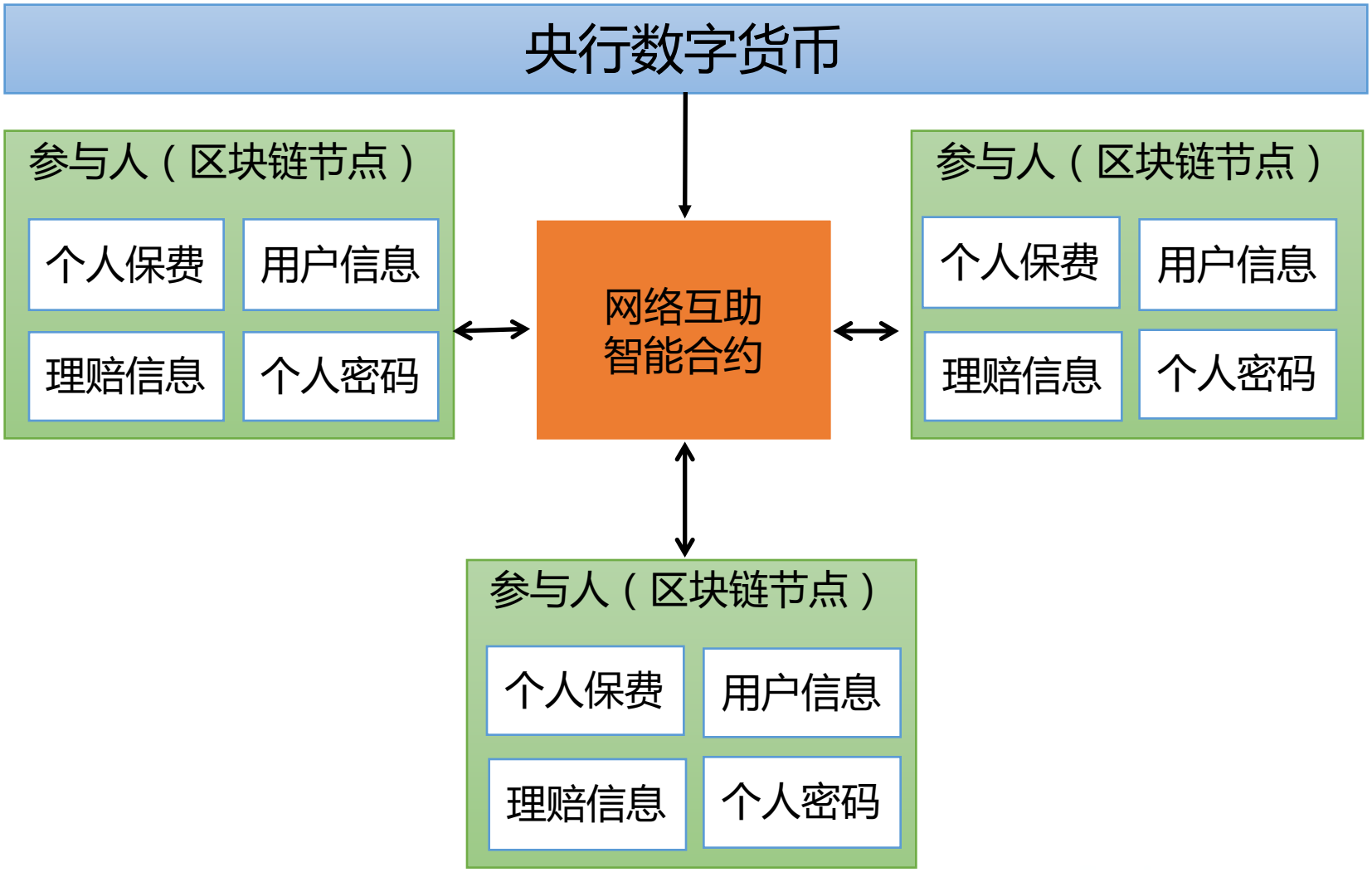
常见的金融应用

互助保险

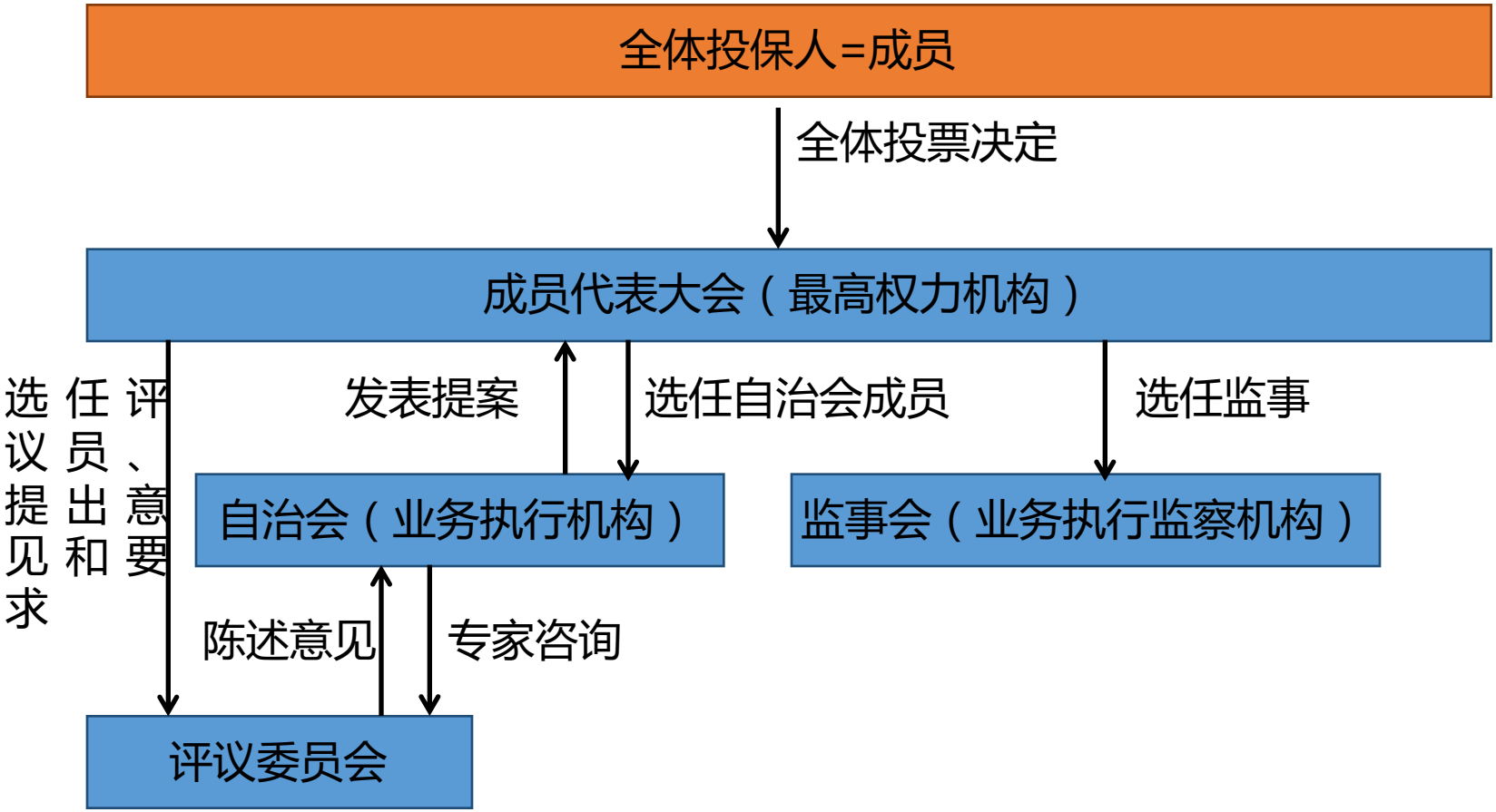
盈利型保险公司

风险共担 经济互助

互助保险


央行数字货币
参与人（区块链节点）
个人保费
用户信息
理赔信息
个人密码
网络互助
智能合约
参与人（区块链节点）
个人保费
用户信息
理赔信息
个人密码
参与人（区块链节点）
个人保费
用户信息
理赔信息
个人密码

所有信息管理如投票、提案、评议、业务执行等均通过区块链智能合约处理



基于区块链的互助保险

低成本

后付费

后定价

期限碎片化

网络互助不是、不是、不是互助保险

无人监管的资金池，严重违规

无偿付准备金刚性给付

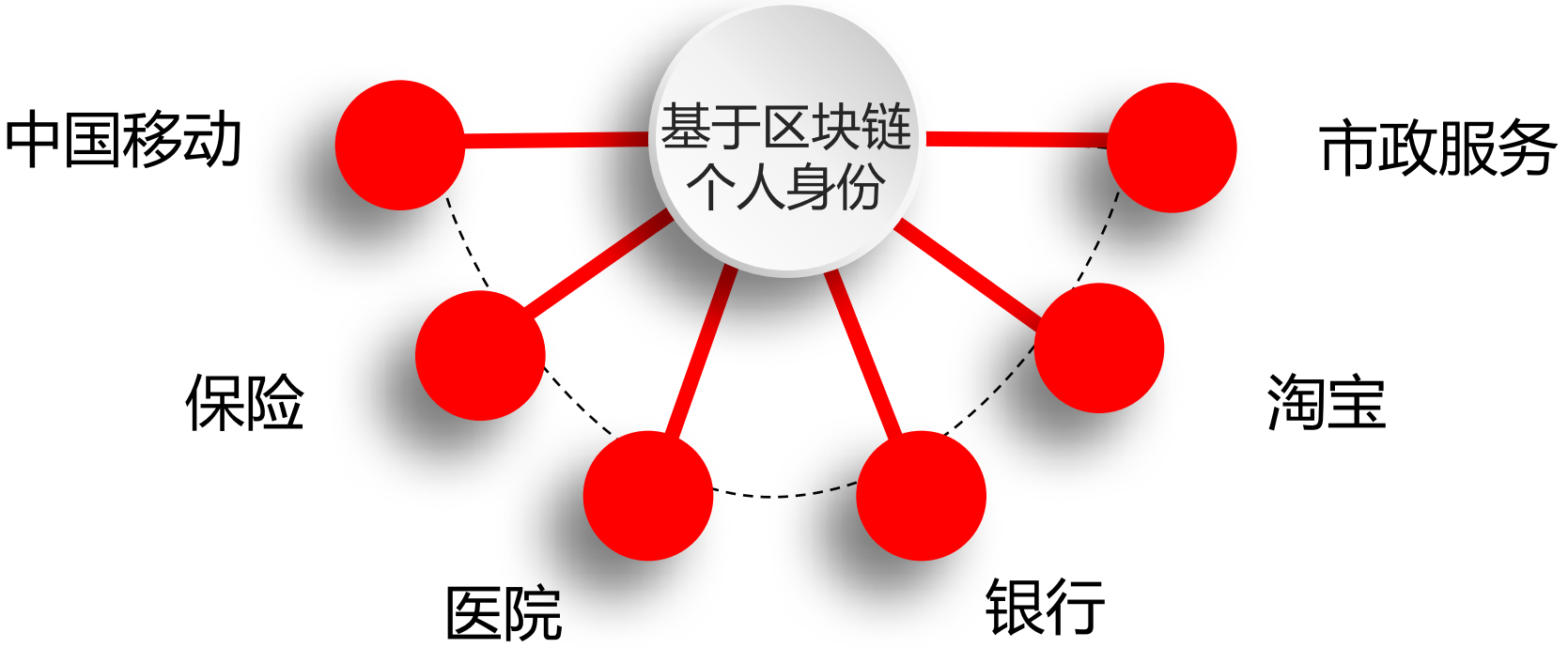
不满足偿付能力监管要求

无刚性兑付能力，无监管兜底，公司倒闭后保单失效

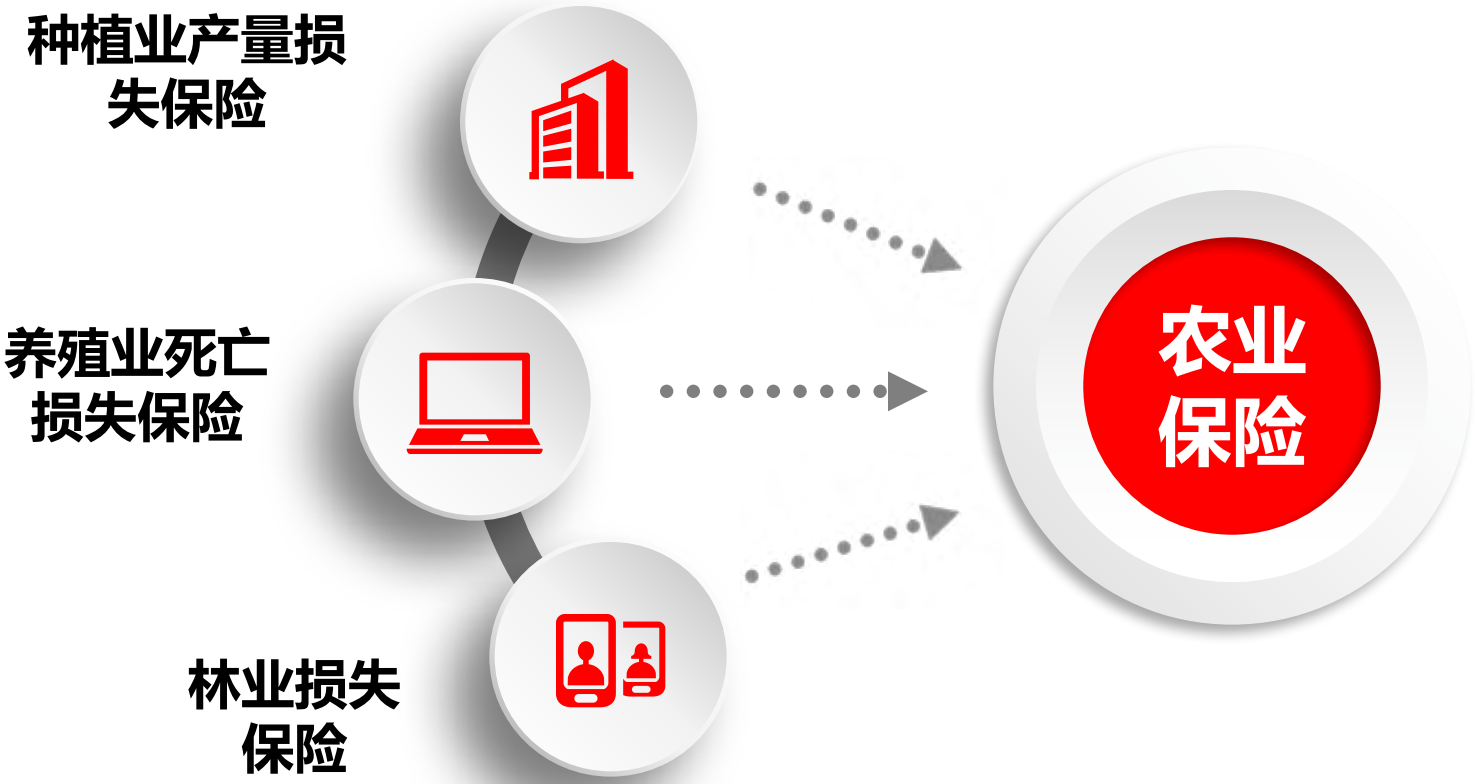
车险信息共享-传统定价模式

车险信息共享-基于区块链

数据属于用户的信用体系



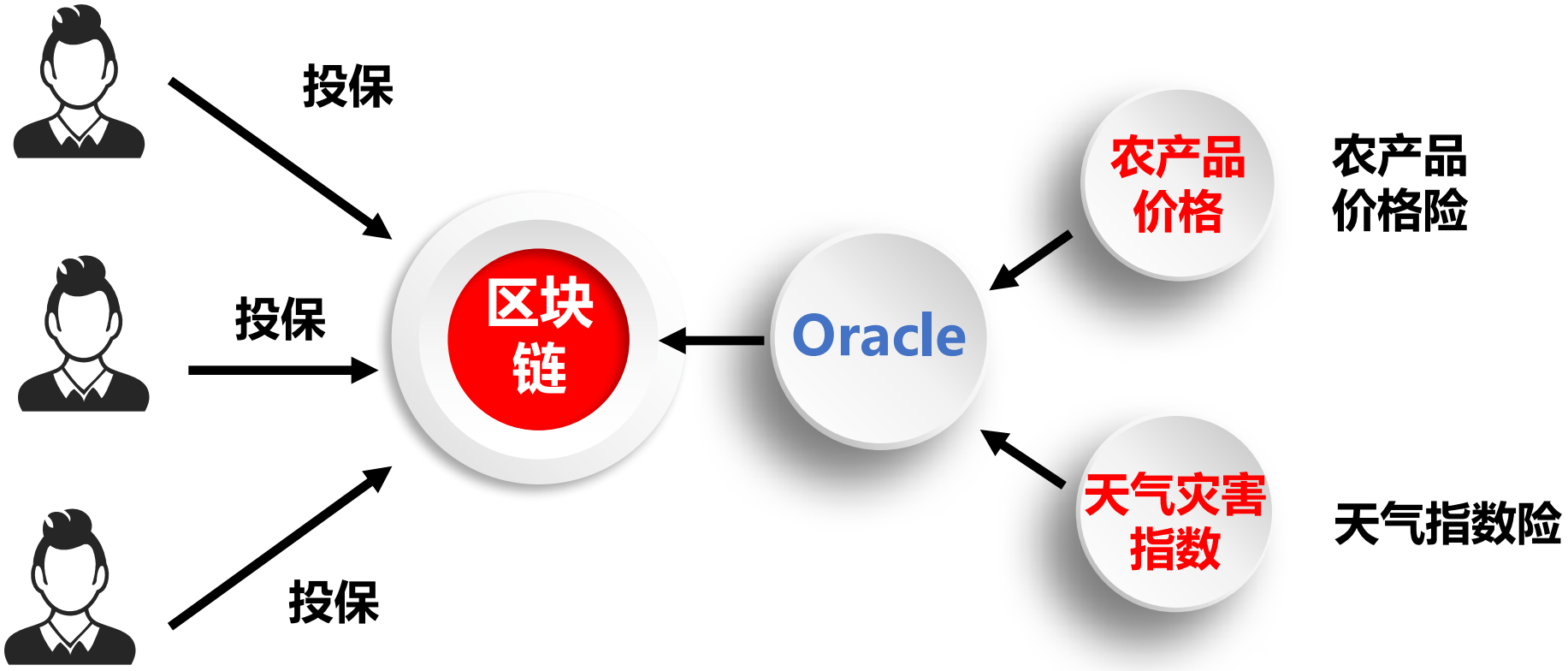
目前农业保险的状态



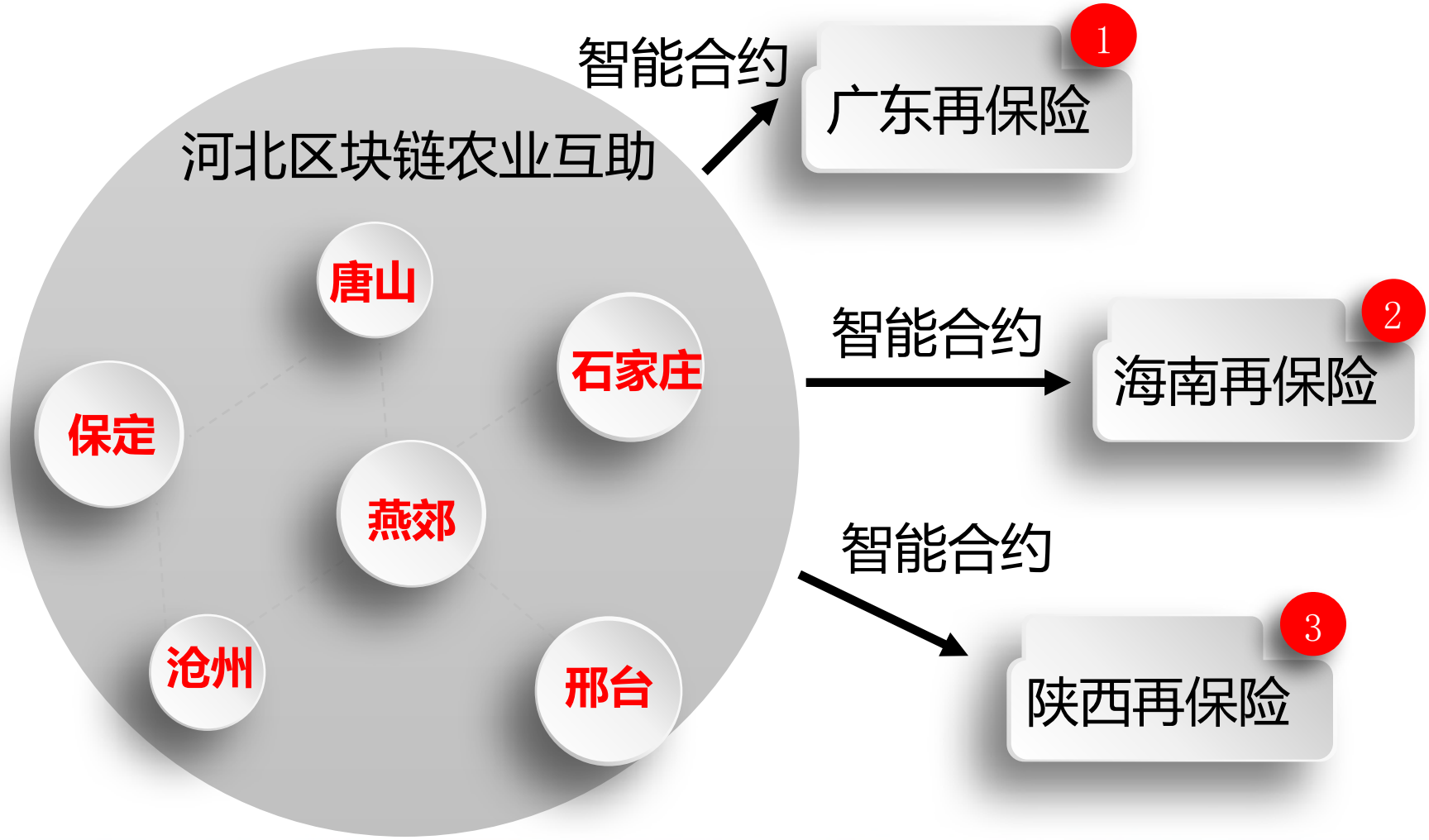
农业保险存在的问题

01	02	03	04
基于一家一户的承包理赔模式	保险条款复杂，理赔流程长，理赔额度少	对损失的产量赔偿，缺少价格暴跌赔偿	理赔人员非专业人士，骗保现象普遍
成本高	农户参与意愿低	保产量不保收入	理赔困难

基于区块链的农业保险



基于区块链的农业保险


河北区块链农业互助
唐山
石家庄
保定
燕郊
沧州
邢台
智能合约
1
广东再保险
智能合约
2
海南再保险
智能合约
3
陕西再保险

04

PART 04

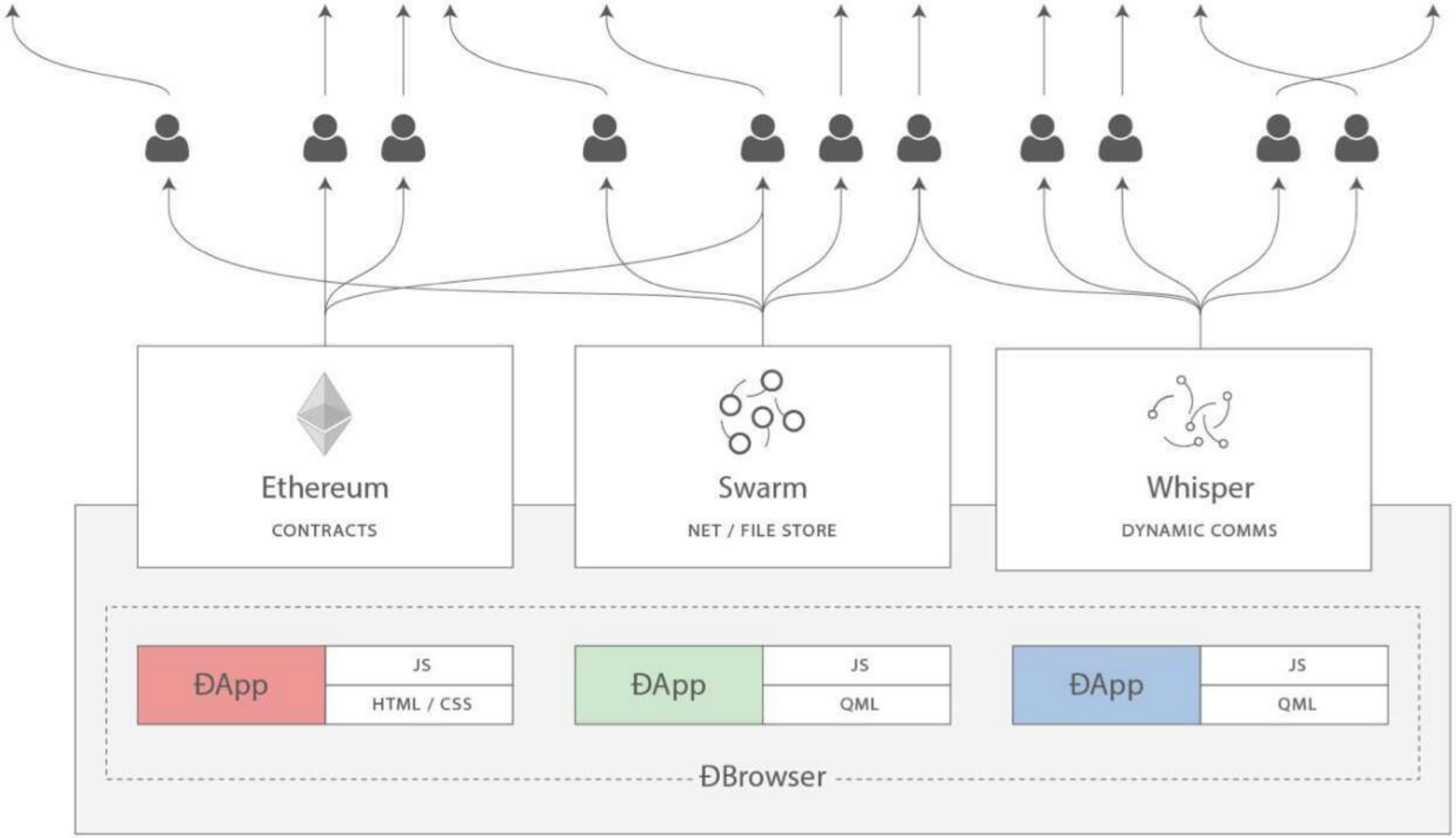
第四部分
去中心化互联网畅想

※ ENS
※ 分片
※ Swarm
※ Whisper

- 数据冗余存储，资源消耗过高
- 无法存储大容量数据
- 链上运算能力极差
- 用户地址过长，使用不便

目前区块链的问题

去中心化互联网畅想


Ethereum
CONTRACTS
Swarm
NET / FILE STORE
Whisper
DYNAMIC COMMS
ĐApp
JS
HTML / CSS
ĐApp
JS
QML
ĐApp
JS
QML
ĐBrowser

ENS-去中心化域名系统

Lihe.eth

0x4B7ef10dFbECe42e55160eeC8a83a6dD86467Fe7

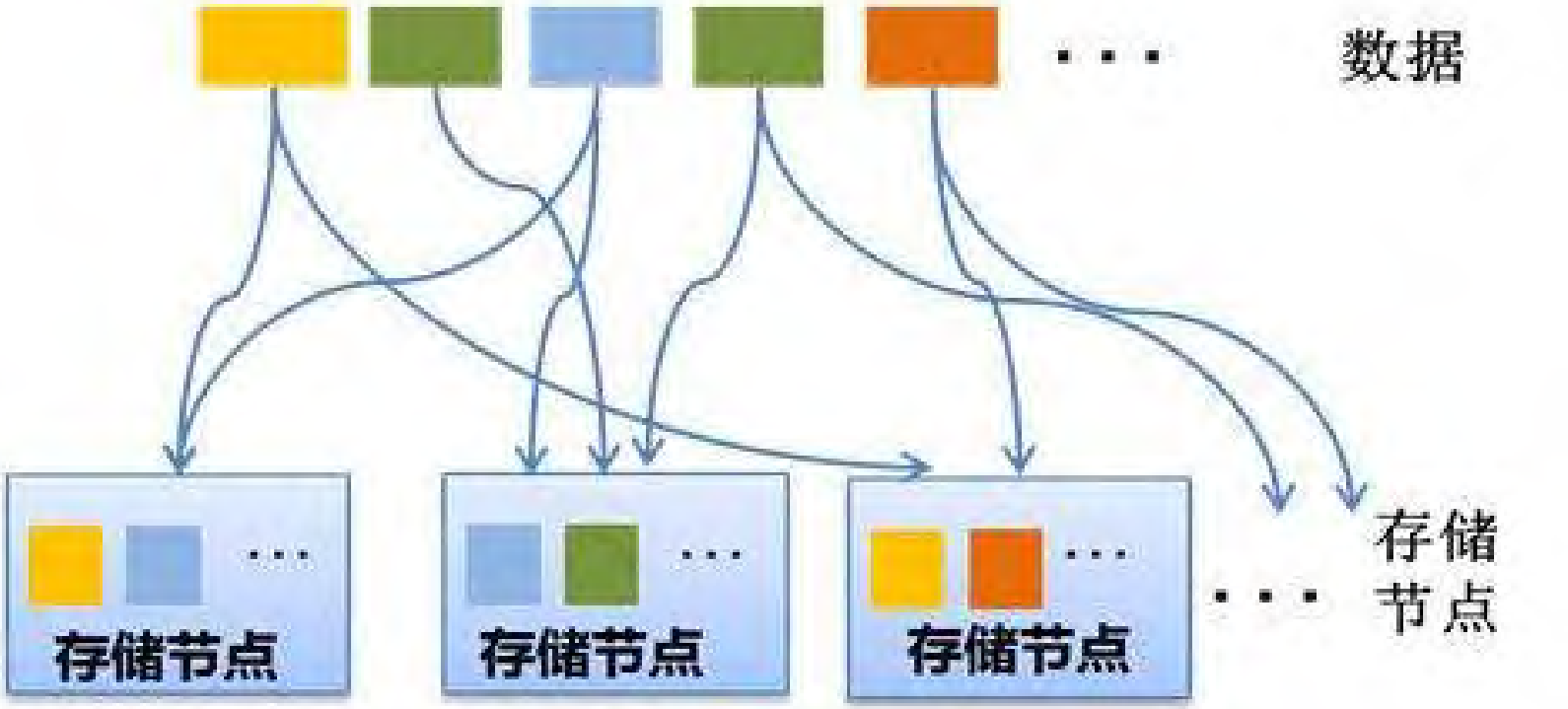
Sharding-分片计算技术

每个挖矿节点都重复计算

每个分片都执行不同的计算

Swarm-去中心化的数据存储服务

bzz:/lihewebsite.eth



Whisper-点对点的消息传输协议

去中心化的互联网

去中心化应用

Swarm、ENS、以太坊、Whisper

云计算公司、云存储公司

中国移动、中国联通、中国电信

感谢倾听!

李赫