WeBank

区块链技术架构与原理解析

2019年7月

区块链是什么

区块链这个黑科技

其实并没有发明什么新的技术

都是成熟技术的组合

区块链知识体系

行业专家

会计 | 支付 | 帐户 | 备付金

机房架构 | 事务处理 | 业务安全 | 前端技术

SDK/API | 智能合约 | 公私钥/签名 | ...

架构师

RPC接口 | ABI编解码 | SSL | 组网搭建

RPC框架 | 区块，交易和回执数据格式 | 区块，交易验证 | Account模型

技术专家

共识算法 | 编译器原理 | 复杂数据结构 | VM机制

P2P网络管理 | 存储技术 | 加密和安全 | ...

金融知识

分布式体系

博弈论

密码学

数据库原理

Java

NodeJs

C++

Go

Rust

Haskell

WeBank

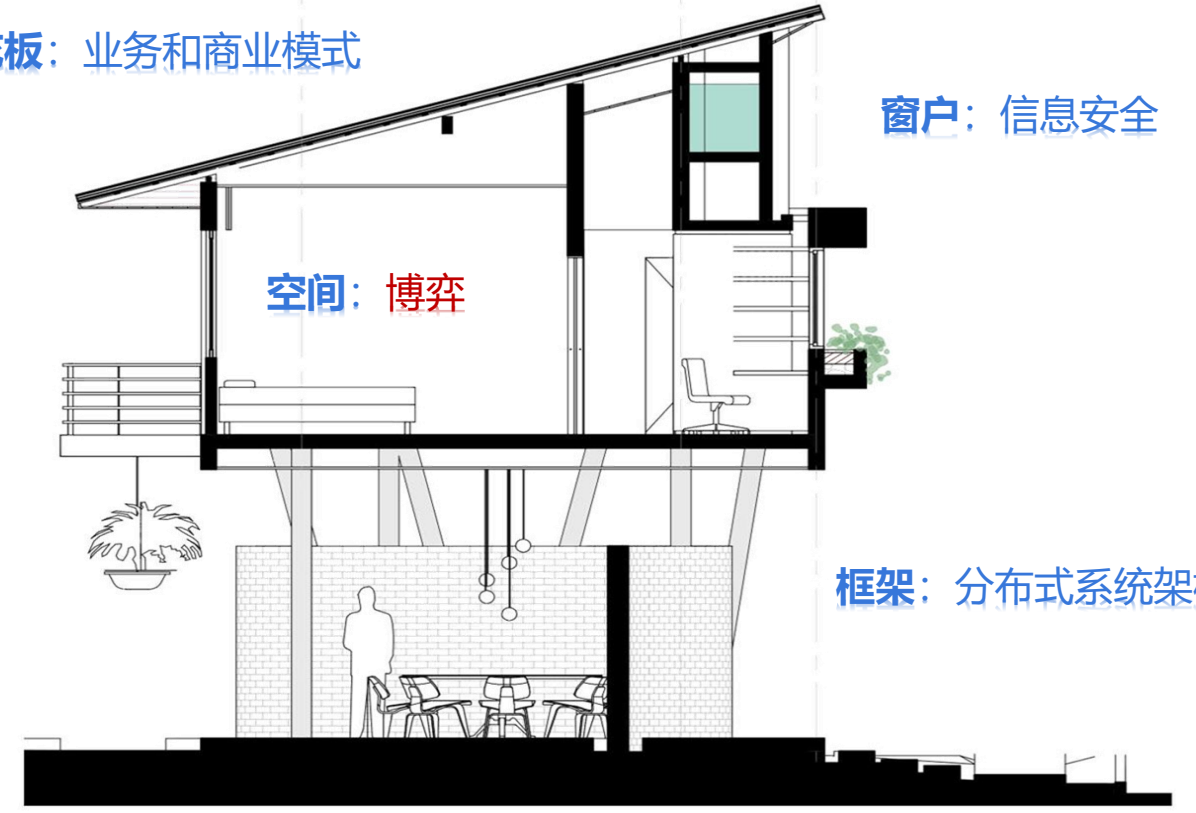
区块链的核心特性

- 结合共识机制和智能合约，进行协同计算和群体鉴证，具有高确定和高可信性，共同构建高效商业模式
- 计算，通信，存储，隐私均进行加密保护，数字签名的运用导致行为无法抵赖
- 独特的链式数据，容易验证和追查，难以篡改，数据具有高一致性，多方冗余存储不怕丢失
- 对等网络通信，多中心，无中介，高效率高可用

一个比喻

天花板：业务和商业模式

窗户：信息安全

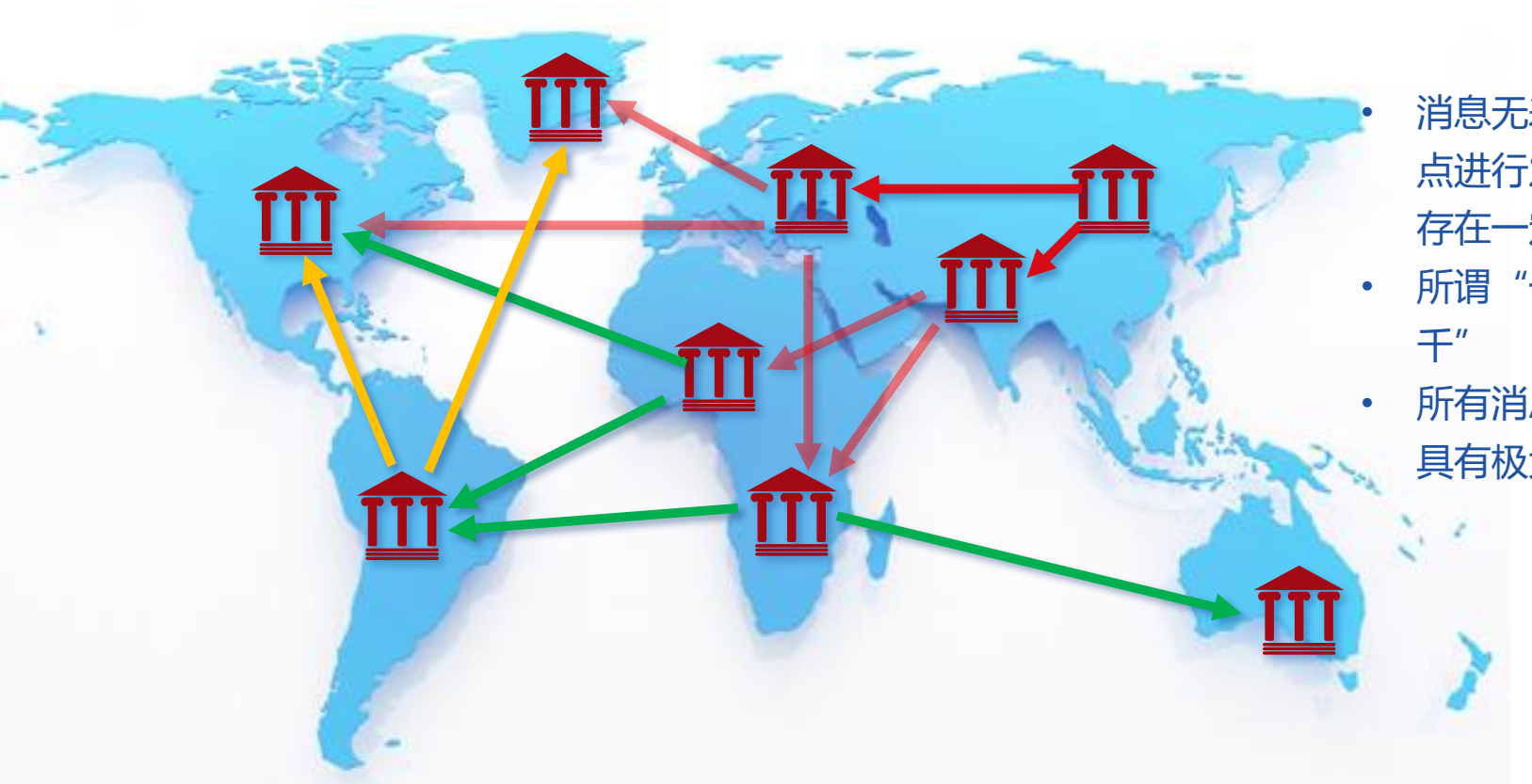


空间：博弈

框架：分布式系统架构

地基：数学，密码学，操作系统，编译原理

网络链：点对点网络里的反复接力传播



- 消息无差别的对自己相邻的节点进行发送，所以称为广播，存在一定的冗余
- 所谓“一传十，十传百，百传千”
- 所有消息通过反复的广播传递，具有极大的概率达到全网

成熟的技术:实现数据的验证和确权

- **哈希(HASH):**表示大量数据的唯一摘要值。原数据的少量更改会在哈希值中产生不可预知的大量更改,可以作为数据的验证凭据
- **数字签名**：信息的发送者（掌握私钥）能产生的别人无法伪造的一段数字串，且可以通过其公布出去的公钥验证是由他发送。

各种数据原文

账目，音视频，证书，合同订单，医疗记录

HASH摘要

HASH:

完整性,正确性

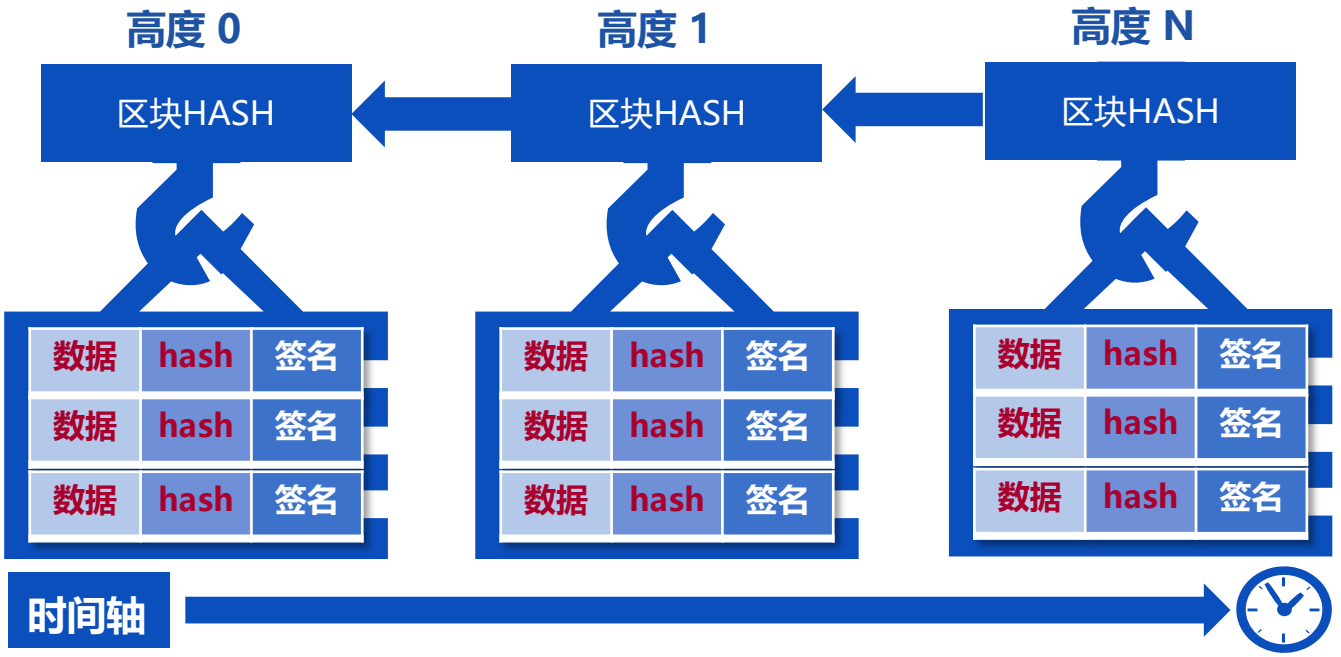
签名 → 验签

数字签名:

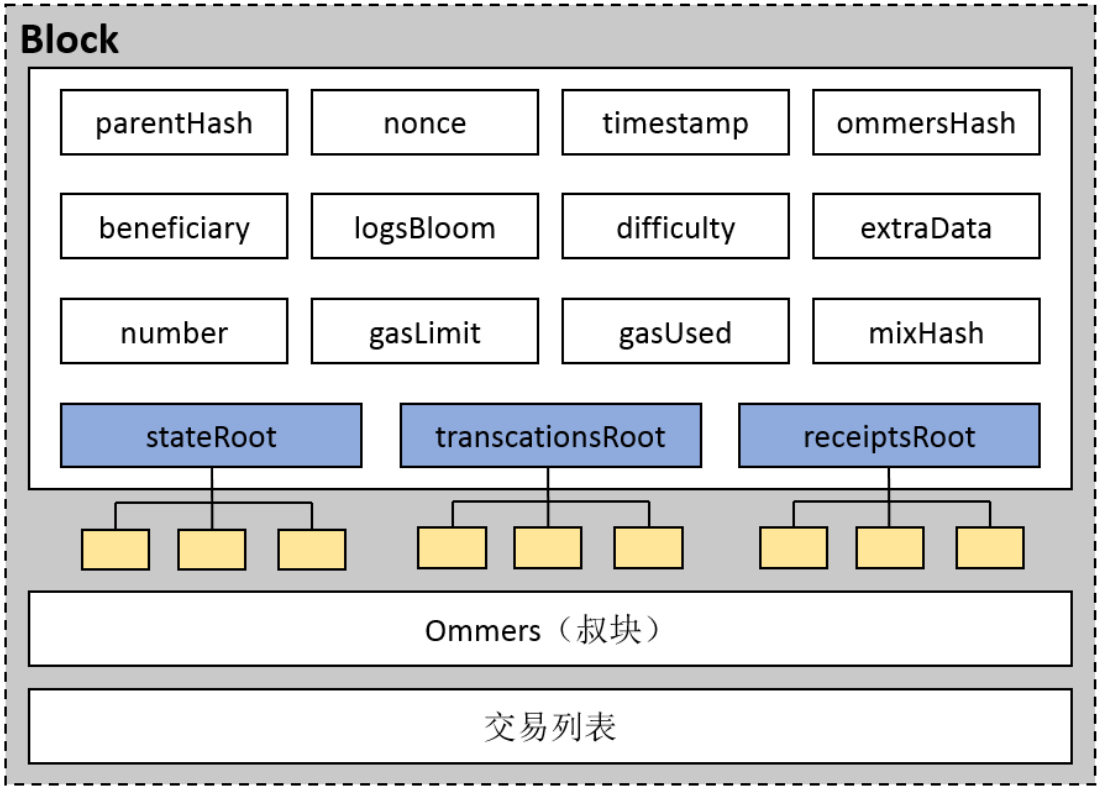
所有者确权

数据链:数据合入区块，区块构成数据链

- 每个区块包含一段时间（如10秒）内产生的交易数据
- 把相关的数据汇总计算摘要，进行汇总的完整性正确性证明
- 每个区块计算摘要时，把前一个区块的摘要做为一个数据计算在内，构成了数据链
- 最新区块包含了所有数据链的完整性证明，整个链条上的任何数据改动都会破坏数据链的相关性

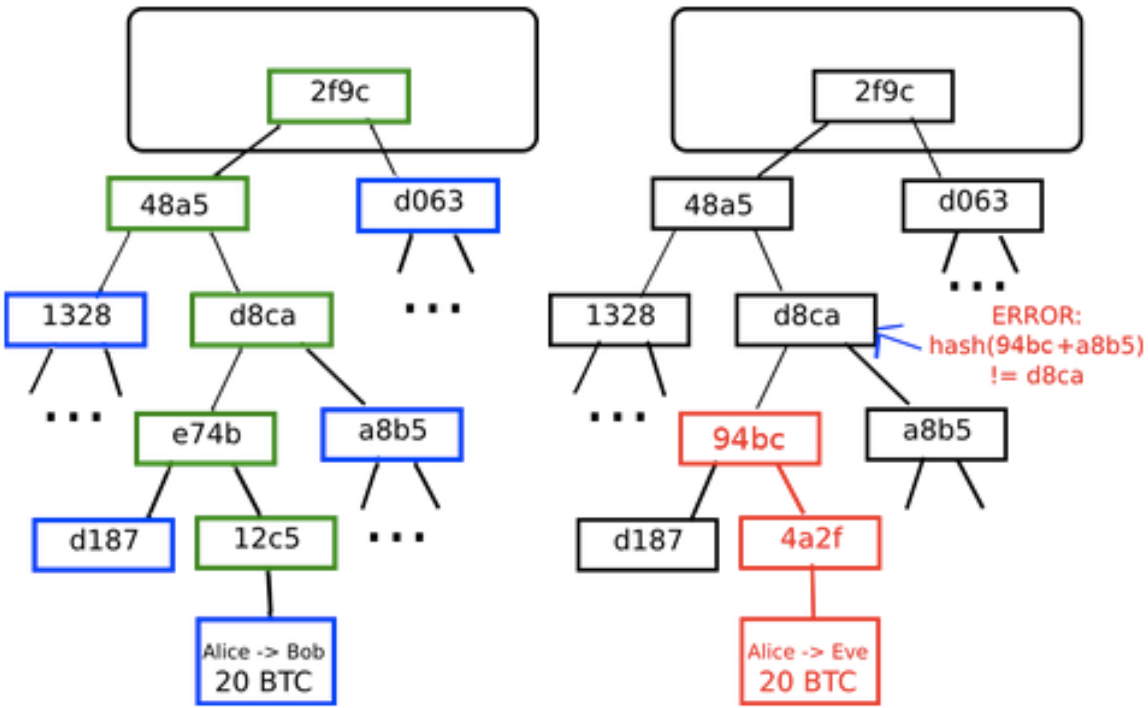


账本结构——区块


Block
parentHash
nonce
timestamp
ommersHash
beneficiary
logsBloom
difficulty
extraData
number
gasLimit
gasUsed
mixHash
stateRoot
transcationsRoot
receiptsRoot
Ommers（叔块）
交易列表

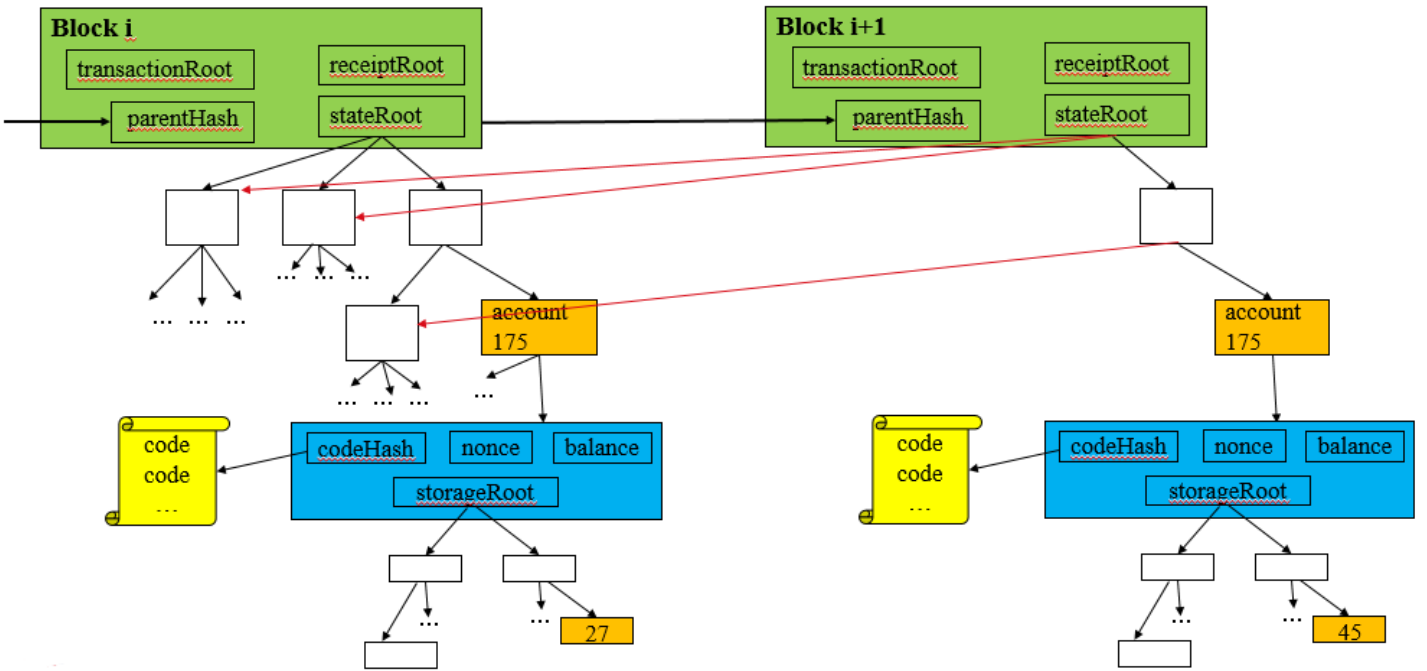
默克尔树

- 默克尔树为区块链状态、交易列表和交易回执列表提供密码学证明
- 通过默克尔树根，轻客户端可以在没有全量数据的情况下，验证区块链状态的部分数据（SPV）



账本结构——state

- 状态(State)
- 以太坊：一个交易驱动的状态机
- Merkle树



账本结构——交易

- 交易(Transaction)类型
  - 转账操作（外部账户->外部账户）
  - 调用智能合约（外部账户->合约账户）
- 交易主要字段
  - Type
  - Nonce
  - Value
  - ReceiveAddress
  - Gas
  - Data
  - VRS

账本结构——回执

- 收据(Receipt)
- 账户创建的交易执行过程中生成的数据
- 收据数据（以及状态数据）不在节点间同步，节点通过执行交易获取
- 主要字段
  - BlockHash & BlockNumber
  - TransactionHash & TransactionIndex
  - From & To
  - CumulativeGasUsed
  - GasUsed
  - ContractAddress
  - Logs

区块链上的记账模型

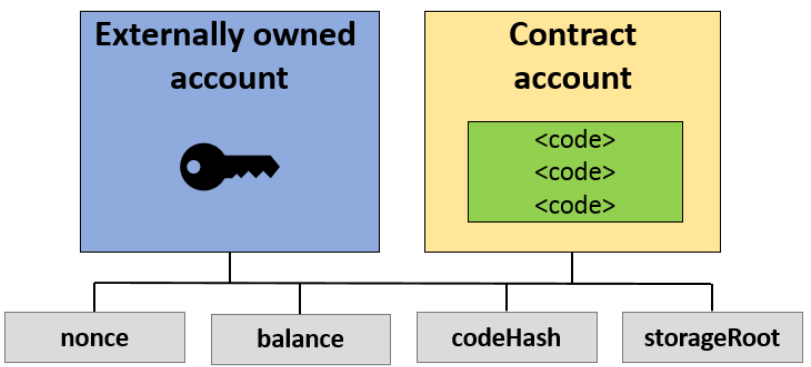
钱包现金模型

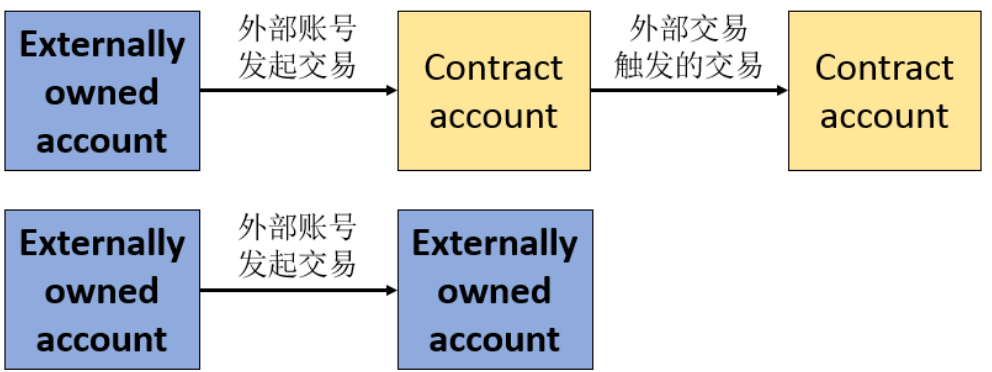
VS

帐户余额模型

账户模型

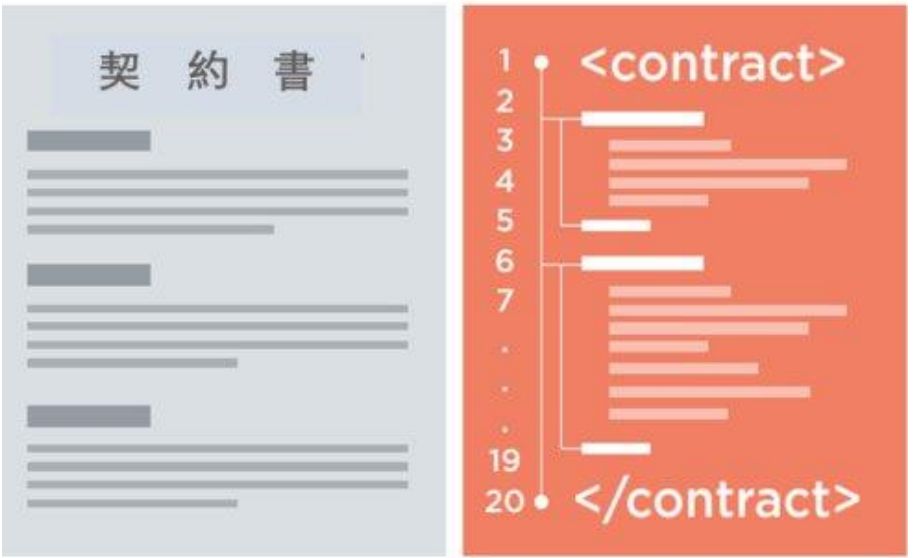
- **账户(Account)**
- **账户的数据组成以太坊全局状态**
- **两种类型**
  - 外部账户(Externally owned account)，私钥控制，没有代码关联，可发起交易
  - 合约账户(Contract account)，合约部署生成，与代码关联，不可发起交易只能被外部账户调用





智能合约的思想

- 将现实世界的逻辑在区块链上实现
- 合约的内容和生命周期被共识确认，是大家认可的条款
- 在所有节点上保证逻辑的一致性
- 在所有节点上产生和维护一致的数据
- 合约还是有可能有Bug的
- “Code is Law”是个理想目标



* 资产管理，合约交易，条件支付，DVP

分层次的开发

用户

User

使用的个人和机构用户

分布式应用

Dapp

有操作交互或应用接口的APP，命令行，网页，手机应用，PC应用等。
和传统应用无区别，通过接口和平台通信

服务接口

API

平台对外提供的标准网络接口，采用通用的JSON格式RPC调用，可以用java, c, go,python,js等语言调用

智能合约

Smart Contract

采用Solidity语言编写，编译部署后可运行，未来可以支持更多的语言

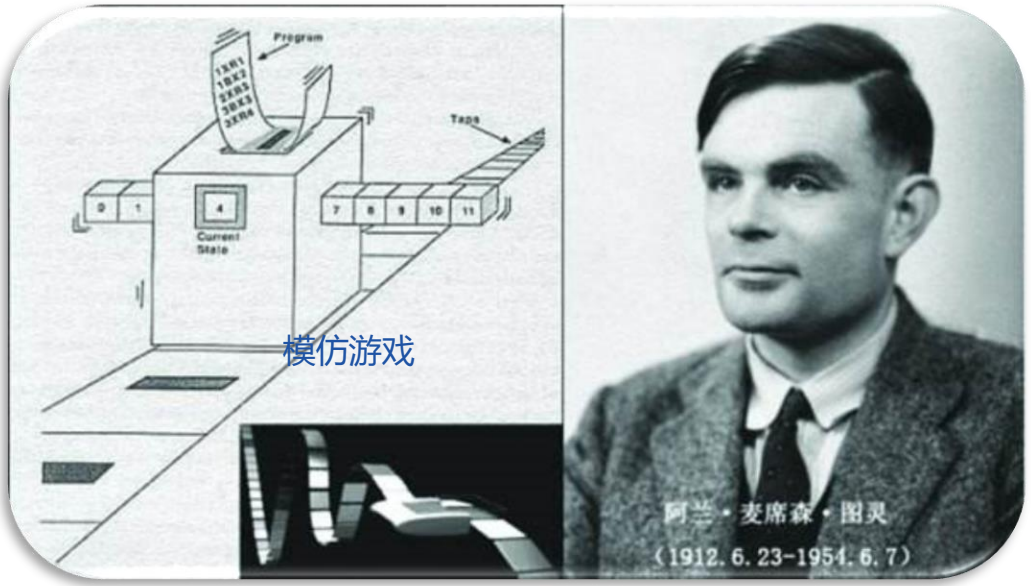
底层平台

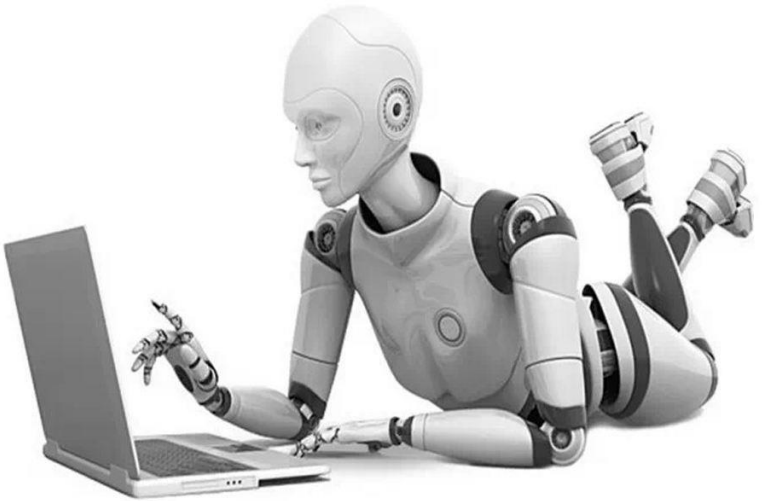
Platform

网络，共识，加密，存储等底层模块

一个图灵完备的语言

- 图灵完备的语言具备强大的可编程能力
- 支持多种数据类型，int，string，map，array
- 支持判断，循环，跳转，分支，且可以应对停机问题
- 支持接口，继承等面向对象的特性

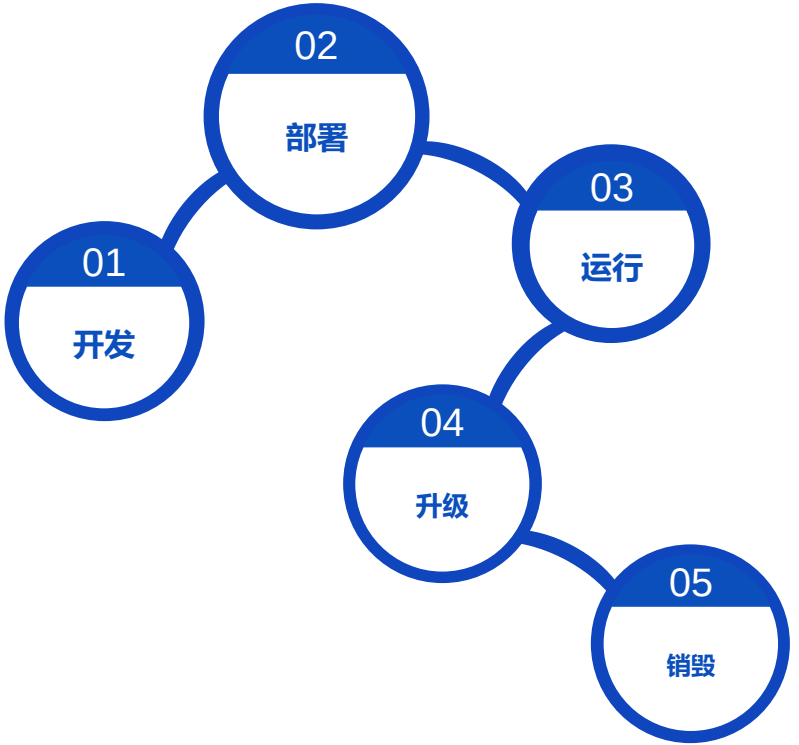




智能合约支持

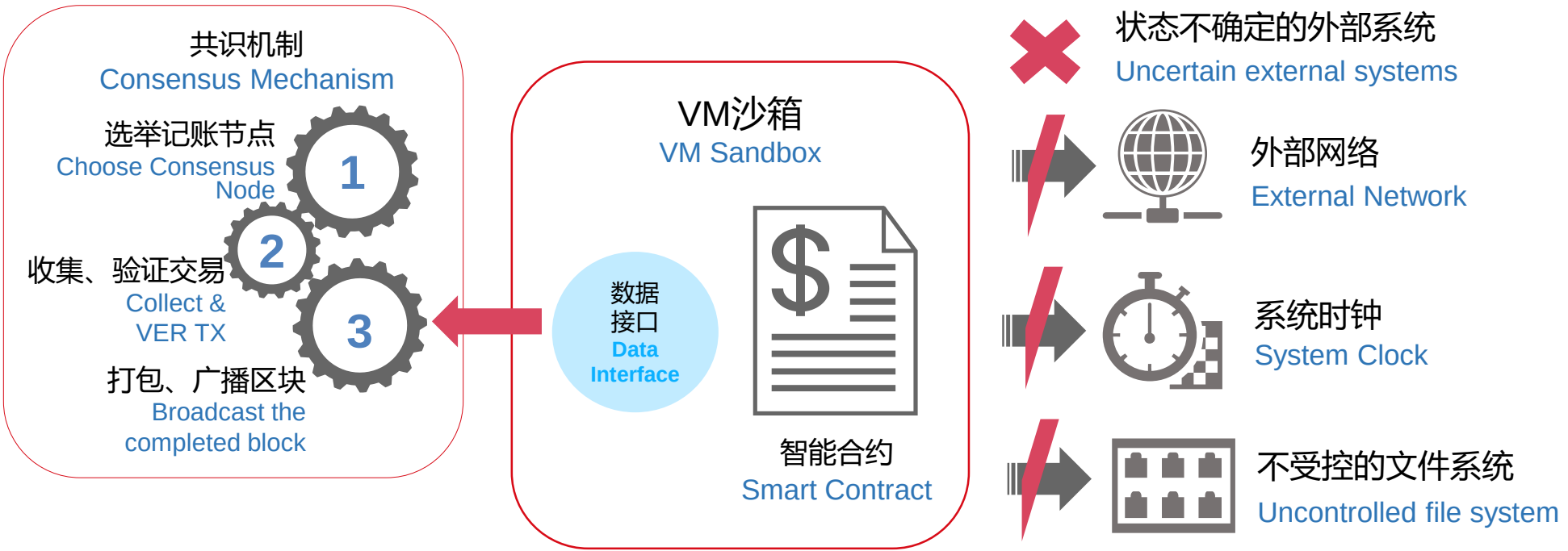
- 使用Solidity语言进行智能合约开发；
- Solidity是图灵完备的高级语言，支持循环、函数调用等用法；
- Solidity拥有丰富的数据类型，支持整形、字符串、数组、Map等；
- Solidity支持继承、库引用等高级用法；
- Solidity拥有大量的参考实现；
- Solidity拥有广泛的开发者；

***智能合约的技术持续进化中，也许会支持更多语言和更强的特性**



数据一致性原理

- 基于联盟链优化的共识机制，共识完成即可确认数据一致性，秒级出块
- 合约在以太坊VM沙箱里运行，不访问外部网络、时钟、文件等不确定性系统，确保运行结果一致性



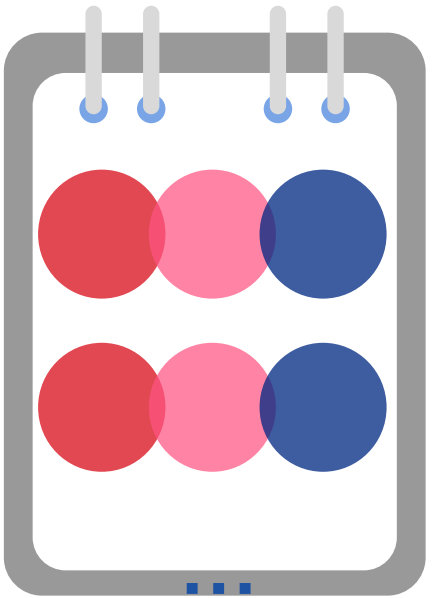
智能合约的用途

功能

数据共享

交易规则

资产管理



身份标识

安全权限

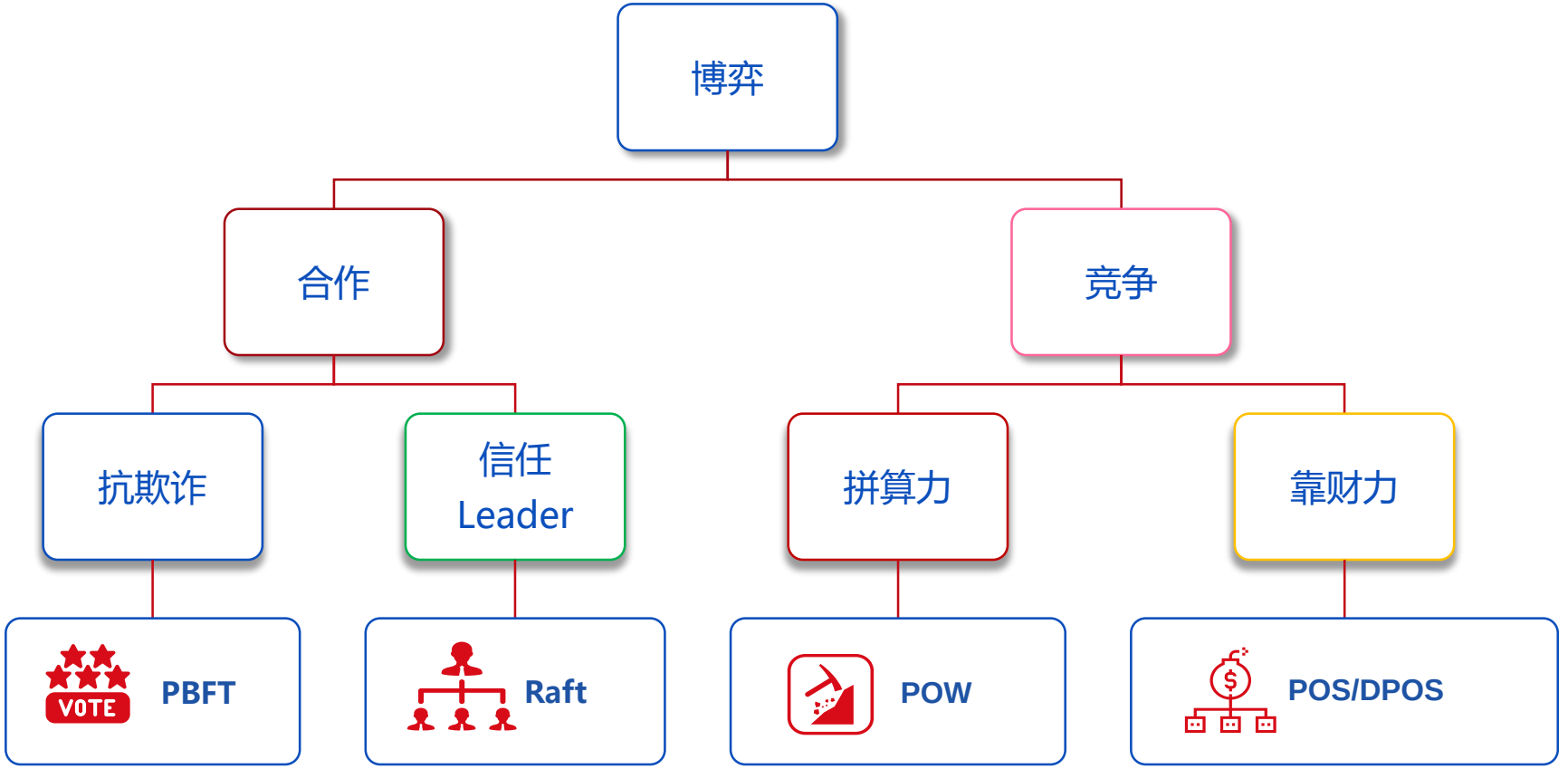
系统配置

治理

共识机制：区块链的核心引擎

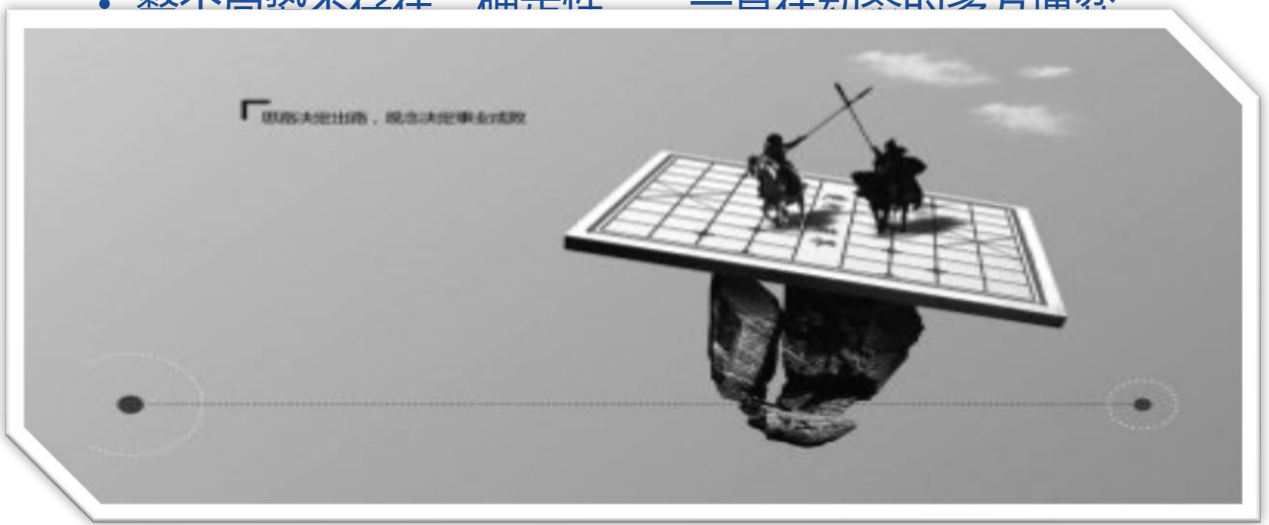
定义：
一种多方协作机制，用于协调多参与方达成共同接受的唯一结果，且保证此过程难以被欺骗，且持续稳定运行。

共识算法的博弈选择

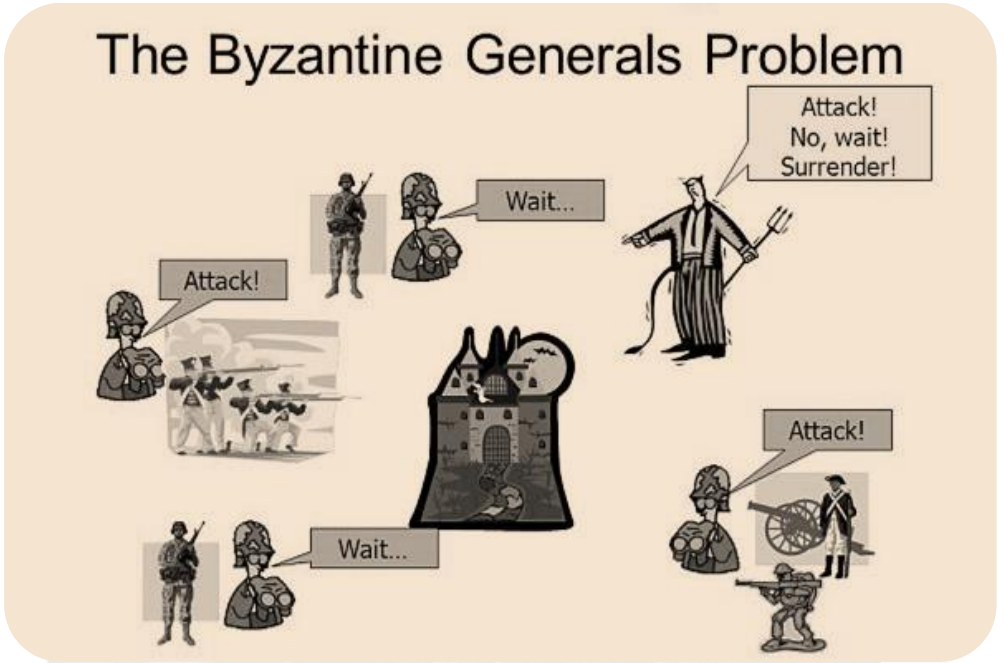


共识模型里体现的的博弈论

- 拥有记账权的人更倾向在维护整个体系过程中获利（纳什均衡+帕累托最优）
- 使用网络的人需要付出一定的成本（手续费、计算费）以免滥用 （避免公地悲剧）
- 少数人作恶的成功几率很低,参考赌徒破产问题（Gambler ‘s Ruin problem）
- 只有极端势力才有可能不顾一切的颠覆这个体系
- 整个局势不存在“确定性”，一直在动态的多方博弈

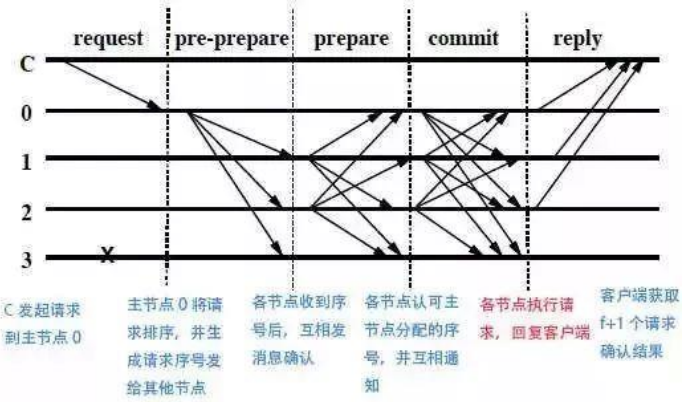


拜占庭将军问题和解决方案(Byzantine Fault Tolerance)



预设条件

- 至少4个以上参与者
- 每轮次有一个发令者
- 少于1/3的参与者作恶或失效
- 极大概率可达的网络（区块链网络）
- 可控的网络规模（少于100参与者）



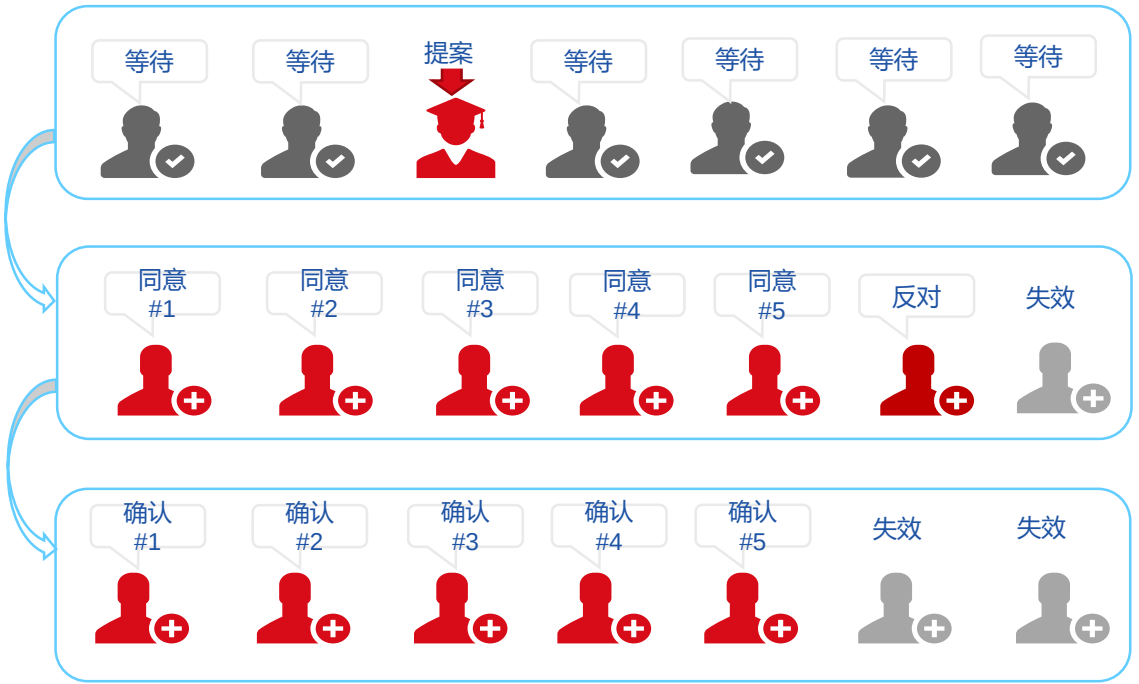
BFT拜占庭将军问题：Lamport，Shostak和Pease于1982年的一篇学术论文中引入, Miguel Castro 和Babara Liskov在1999年提出PBFT，放松了约束来解决拜占庭问题。Liskov于2008年获得了图灵奖

拜占庭将军问题相关的图灵奖得主

Lamport分布式计算理论奠定了这门学科的基础。他在1978年发表的论文《分布式系统内的时间、时钟事件顺序（Time, Clocks, and the Ordering of Events in a Distributed System）》成为计算机科学史上被引用最多的文献。他为“并发系统的规范与验证”研究贡献了核心原理。

2008年，美国计算机协会(ACM) 宣布Barbara为当年年度图灵奖获得者，以表彰其在程序设计语言与系统设计，特别是在数据抽象、容错和分布式计算领域的实践和理论基础方面的贡献。

一次PBFT协商过程:民主集中制



(提议：本小组周二上午开会)

确认记账者列表,每一轮次选出新的提案人,提案人排序打包，广播提案

(投票：周二上午开会,同意/反对/不表态)

所有记账者针对提案进行检验（检查交易，运行合约等），都通过的话发出同意投票，超过2/3进入下一轮

(确认：大家设定日程，并反馈参加确认消息)

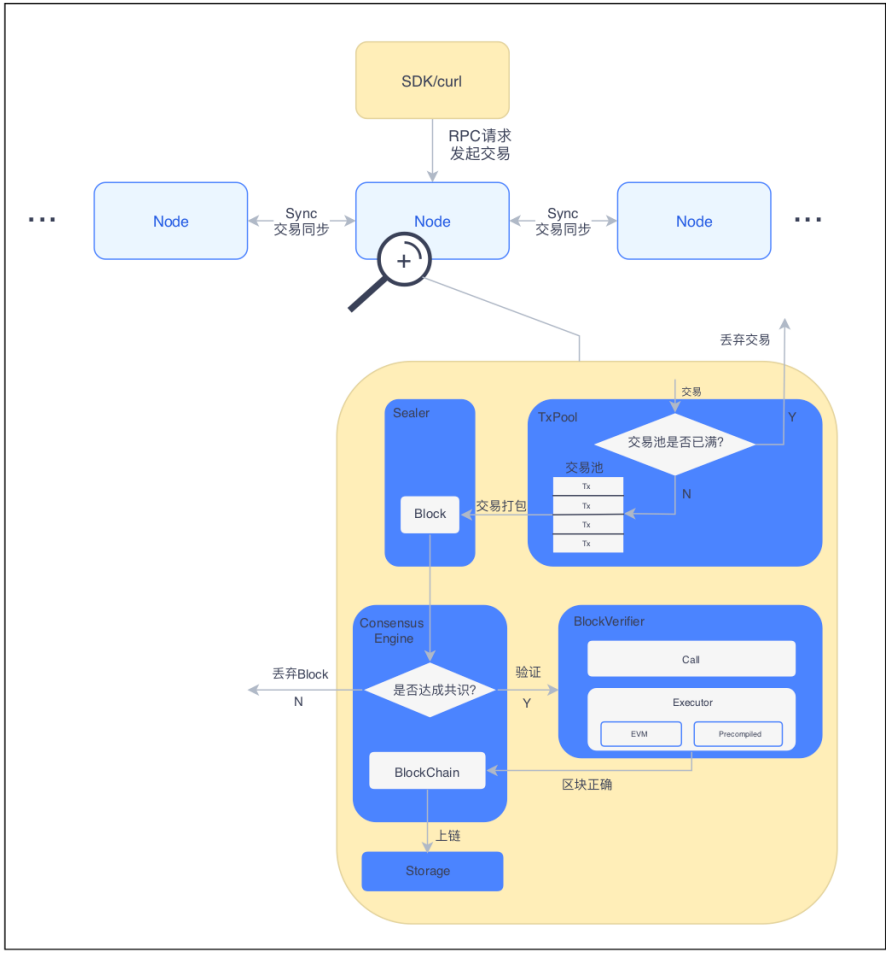
所有记账者表示可以收妥提案，如果超过2/3人表示收妥，则提交存储，进入下一轮

- 实际的处理过程**非常复杂**，需要考虑：

公平高效的选出记账者列表 | 议长轮换和存活检测 | 超时进行轮次切换
共识时间 | 网络波动 | 广播流量 | 交易计算量 | 区块同步校验
过多节点不共识 | 网络规模太大 | 极端情况下的崩溃恢复

交易处理概要流程

- 一个完整的交易流涉及多个模块：
  - 接入模块
  - 共识模块
  - 存储模块
  - 网络与同步
  - 交易执行器
  - 安全控制

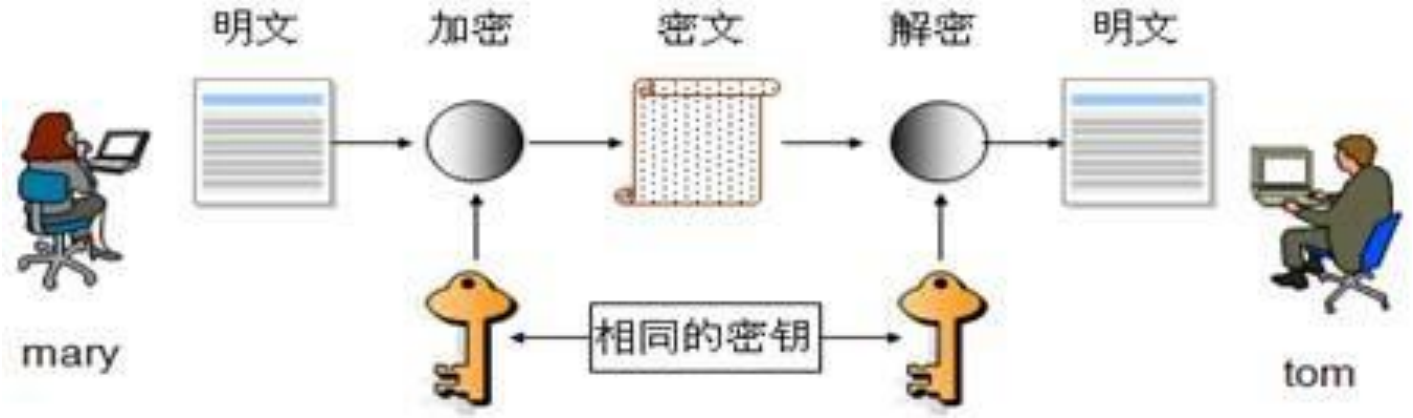


密码学基础

对称加密

使用相同的密钥

加密大量数据



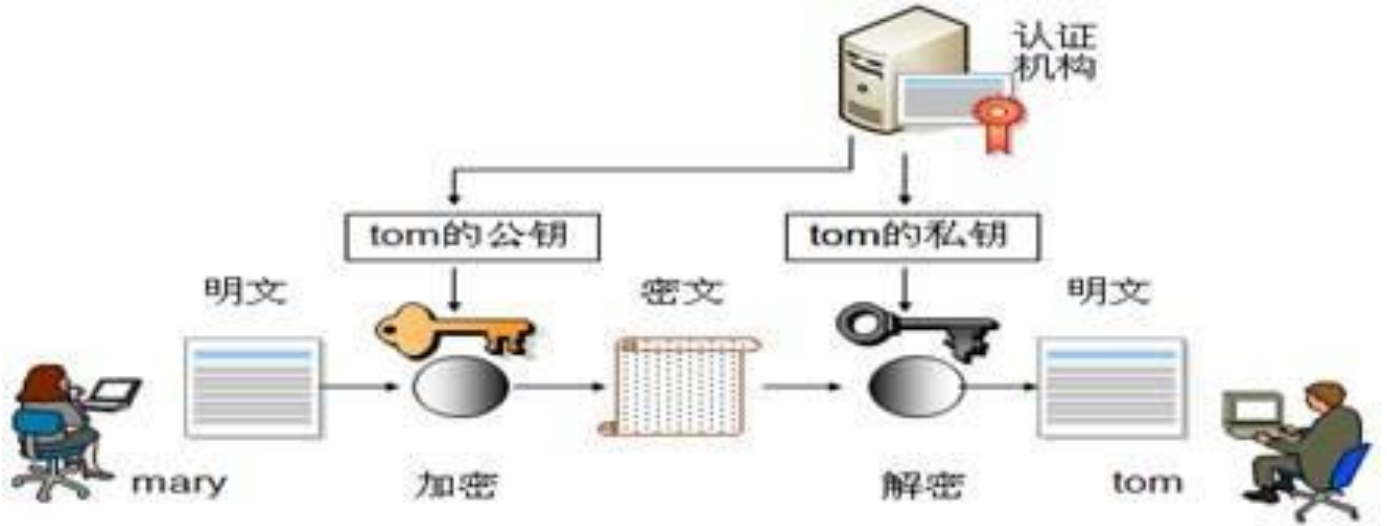
非对称加密

采用不同的密钥

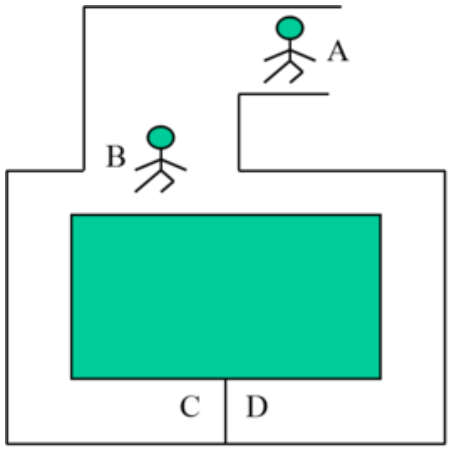
加密少量数据

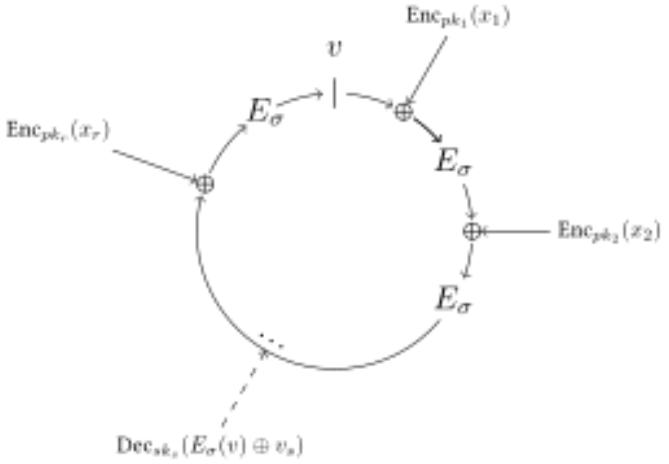
用于交换对称密钥

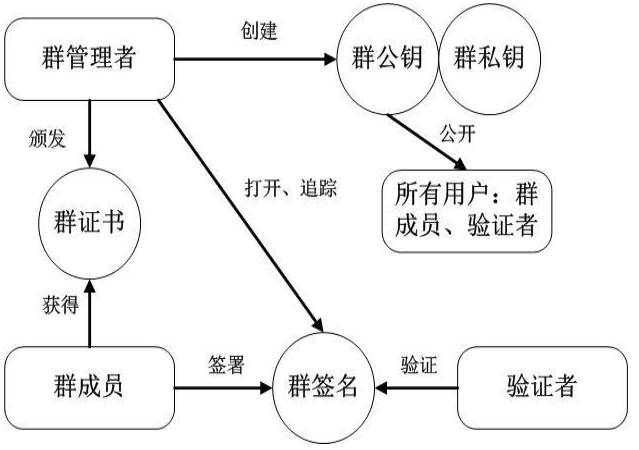
用于签名验签



博大精深的密码学算法







- 零知识证明
- 同态加密
- 属性加密，格密码学
- 群签名，环签名，盲签名、代理签名、门限签名…
- 量子密码

区块链不能一锤子解决的问题

鸿沟：物理世界的资产无缝追溯，如纸质发票，纸质证书，房产，仓储

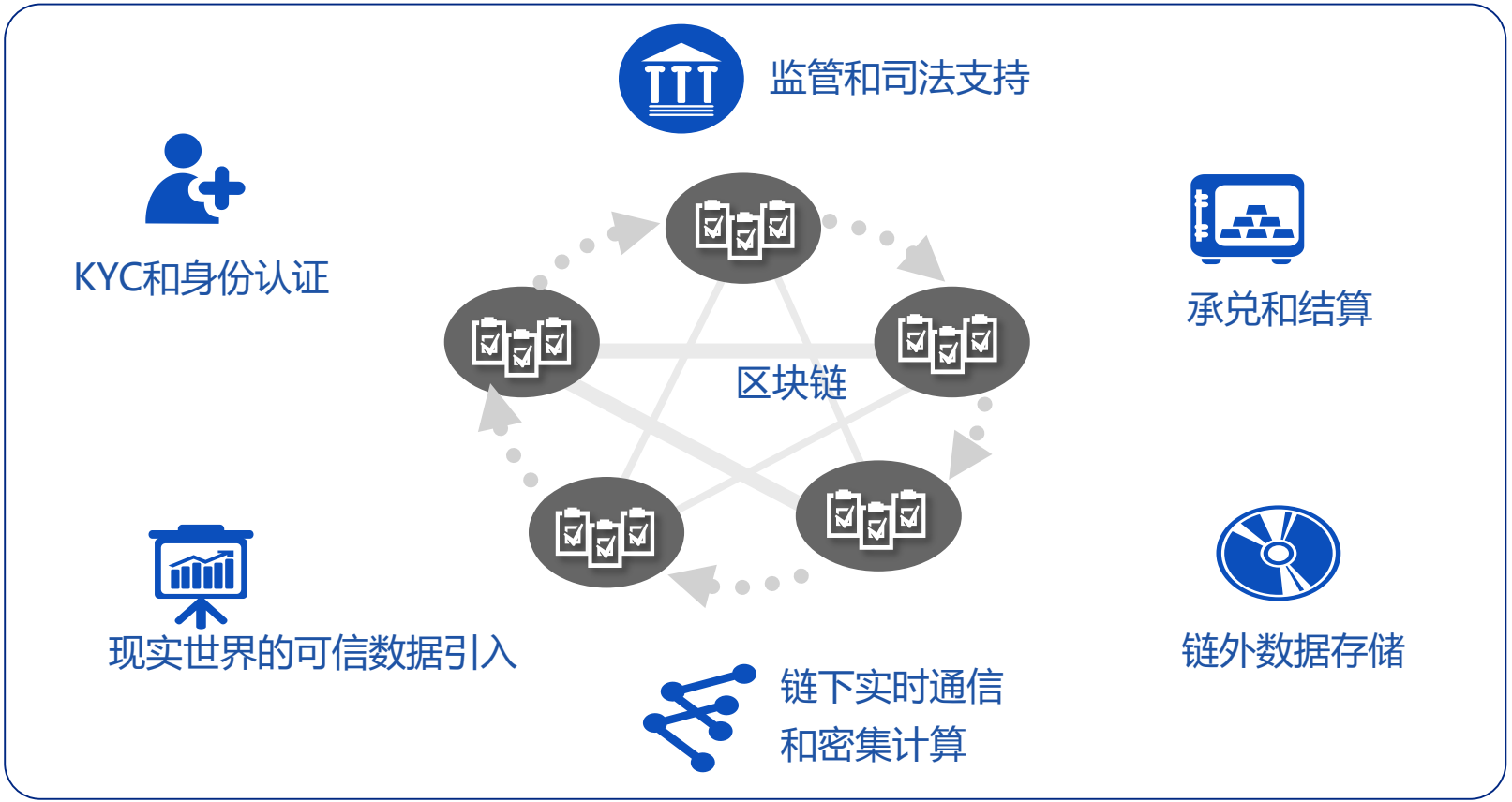
容量：保存大容量数据，需要依赖链外存储，如视频、图片、大数据原文

计算：高度实时低时延的交易往来，或者高强度的计算如大数据分析

安全：安全和隐私导致额外的复杂度，且未必能满足银行级安全标准

中心：呈现强中心化特质的业务关系

区块链需要“混合架构”


监管和司法支持
KYC和身份认证
区块链
承兑和结算
现实世界的可信数据引入
链外数据存储
链下实时通信
和密集计算

FISCO BCOS——集实践大成的开源底层平台

- 由金链盟开源工作组进行规划和开发，针对金融行业的监管合规与特定业务需求；
- 打造安全可控的区块链底层平台，完全对行业开源；

社区群管理员

金融区块链平台FISCO BCOS

开源社区GITHUB网址

微众银行/金链盟区块链开源产品：Please Star

- **WeIdentity：实体身份标识 x 可信数据交换**
  - https://github.com/WeBankFinTech/WeIdentity
- **WeEvent：基于区块链的事件驱动架构**
  - https://github.com/WeBankFinTech/WeEvent
- **WeBASE：区块链中间件平台**
  - https://github.com/WeBankFinTech/WeBASE
- **FISCO-BCOS：**
  - https://github.com/FISCO-BCOS/FISCO-BCOS

WeBank

谢谢！