WeBank

课程回顾及思考

2019年7月

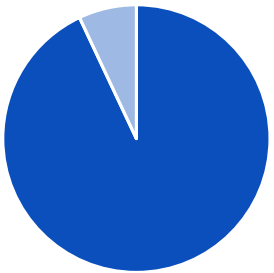
FISCO金链盟

01

课程回顾

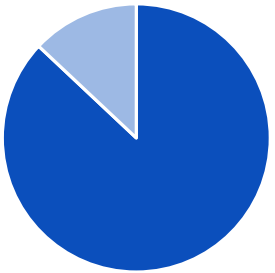
公链发展及现状

比特币 Bitcoin



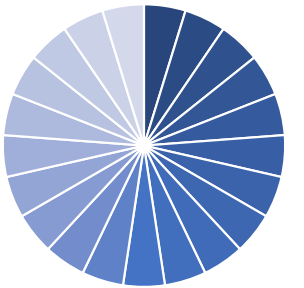
前10大矿池算力合计超过93%

以太坊 Ethereum



前10大矿池算力合计超过87%

EOS



由21个超级节点联合记账

技术选型：联盟链

- 共识机制与技术信任
- 可信数据与分布式账本
- 加解密与隐私保护算法
- 分布式对等网络
- 智能合约

联盟链

- 准入机制
- 监管节点
- 身份认证
- 去代币

VS

公有链

- 虚拟代币
- 挖矿激励
- 匿名交易

我们的选择：联盟链，兼顾金融创新与金融稳定

- 区块链作为一种整体技术解决方案，融汇吸收了分布式架构、分布式存储、点对点网络协议、加密算法、共识算法、智能合约等多类技术
- 联盟链作为支持分布式商业的基础组件，更能满足分布式商业中的多方对等合作与合规有序发展要求

FISCO-BCOS：开源联盟链底层平台

- 国内企业主导研发、对外开源、安全可控的企业级金融联盟链底层平台
- FISCO BCOS代码仓库
  https://github.com/fisco-bcos
- FISCO BCOS开源社区

开源生态：应用落地

区块链应用案例集

FISCO-BCOS演进之路

方案设计

2017.01-2017.03
技术选型：联盟链
基于BCOS重塑升级

平台研发

2017.04-2017.10
核心算法研发
底层架构研发

应用实践

2017.08-2017.11
完成一个应用研发
验证底层系统可用性

开源发布

2017.12
在Github完全开源

生态建设

2017.12-～
组建千人规模的社区
数十个应用落地

举办大赛

2018.08-2018.12
近300支团队报名参赛
覆盖十几个行业领域

架构升级

2019.01-2019.03
全新2.0架构升级

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

架构师

技术专家

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	…
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
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

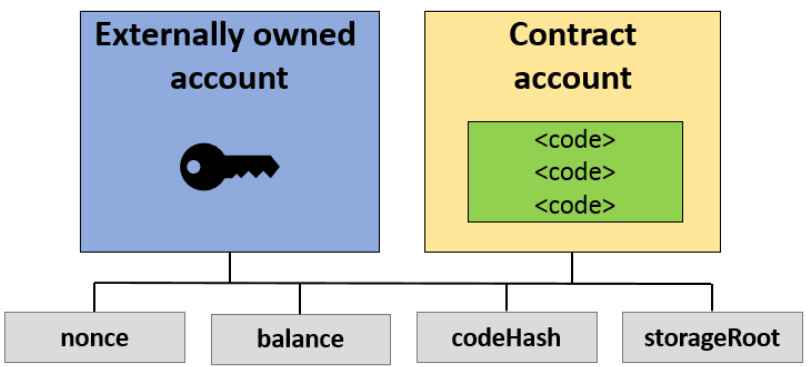
- Java
- NodeJs
- C++
- Go
- Rust
- Haskell

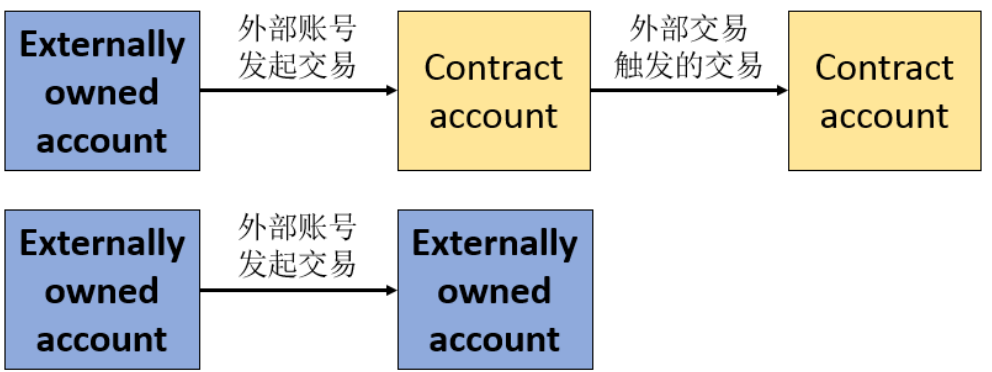
区块链的核心特性

- 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

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

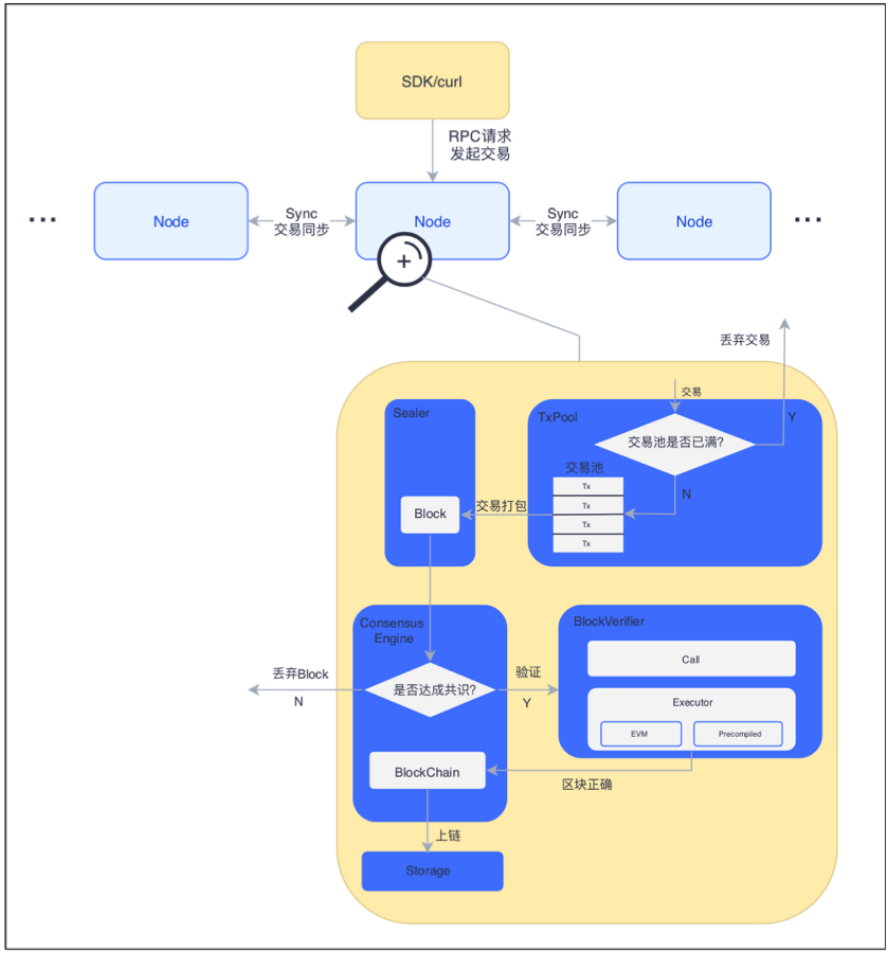




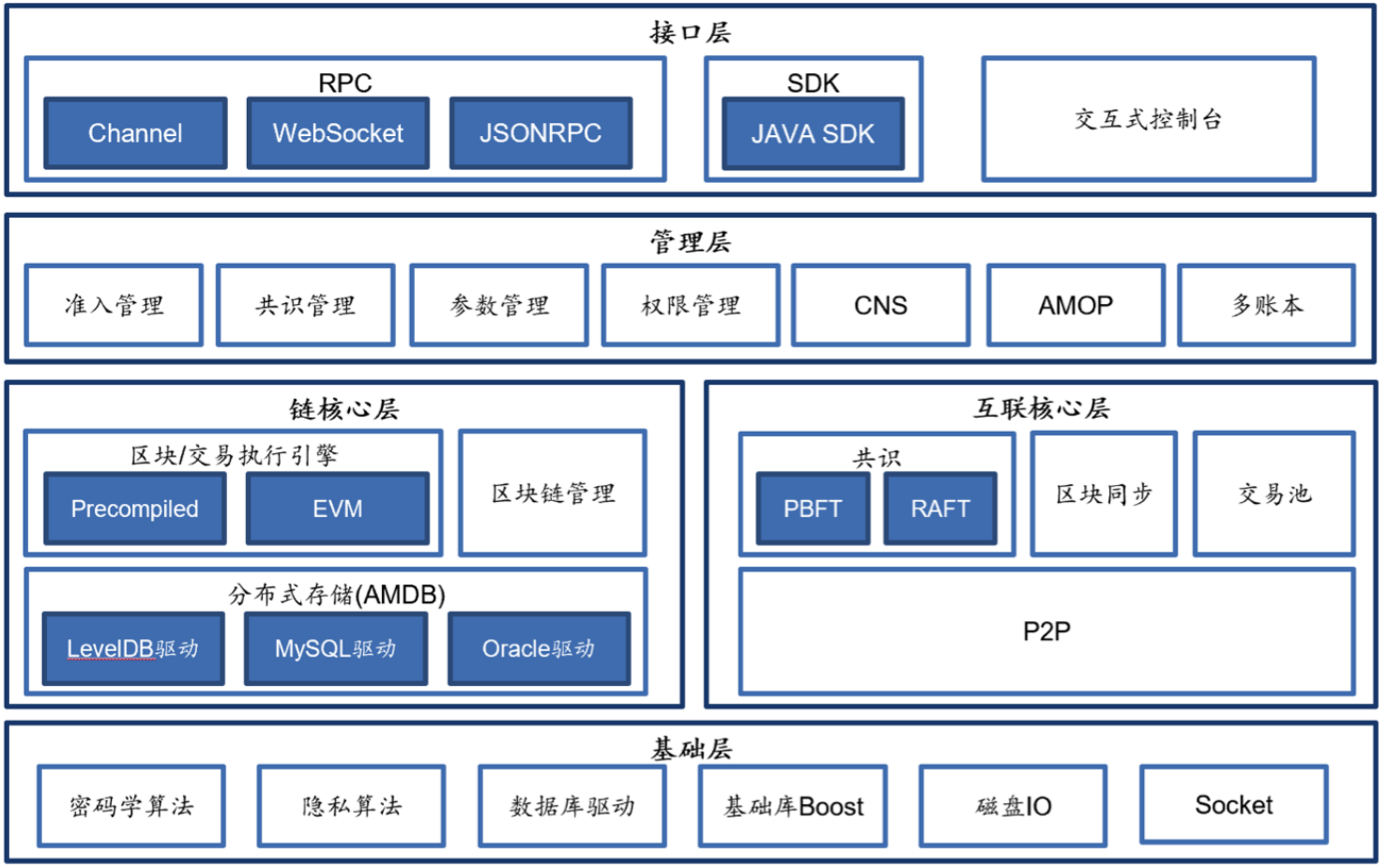
交易处理概要流程

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



FISCO BCOS 逻辑架构



FISCO BCOS 2.0

技术要求

What kind of technology do we need

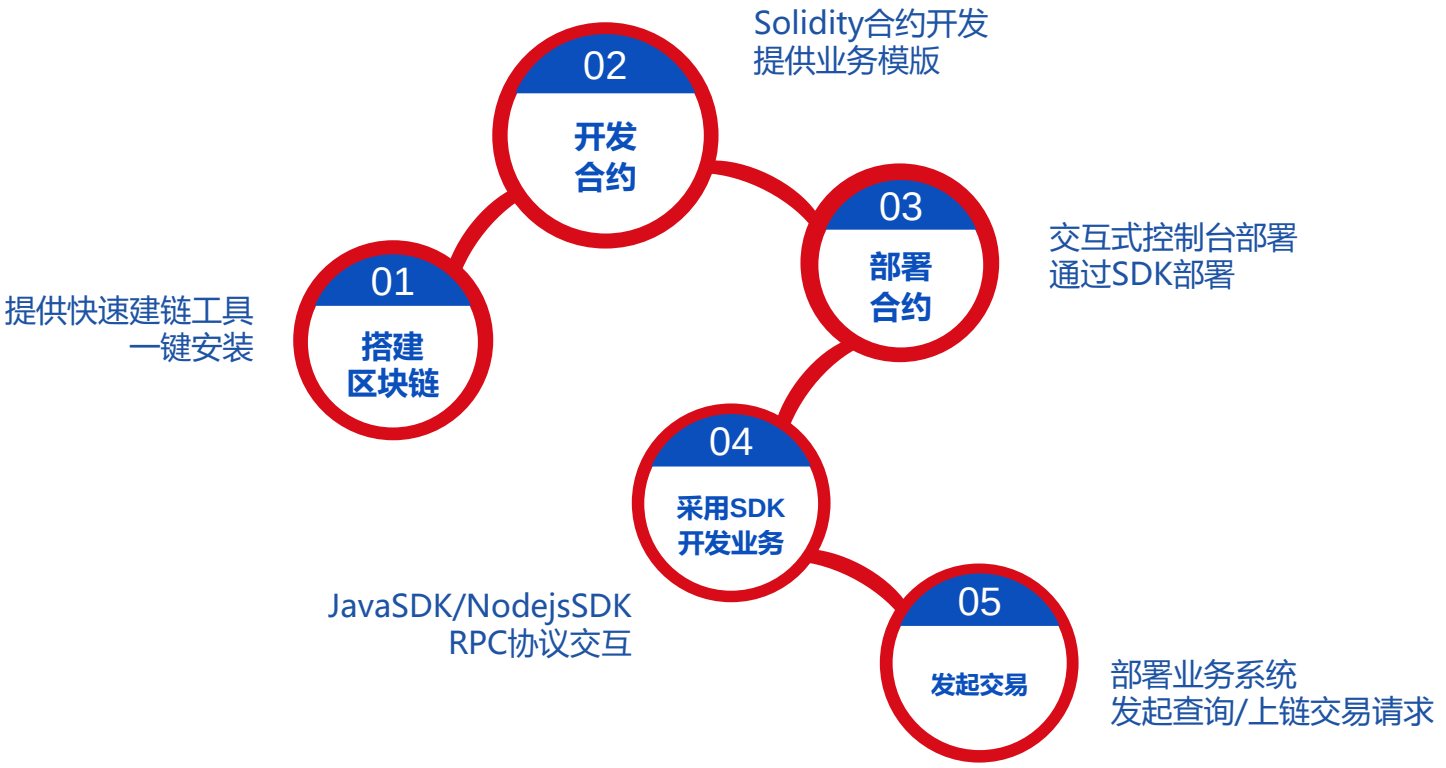
- 支持快速组建联盟和建链的能力，让企业建链像建微信群一样简便
- 具备高可用的多群组能力，能处理海量服务请求
- 具有良好的联盟链治理能力，满足企业级运维管理要求
- 具有可行的隐私保护能力，能支持复杂业务需求落地
- 开源和开放，实现联盟成员之间的充分信任

.0 新特性

at 's new in FISCO BCOS 2.0

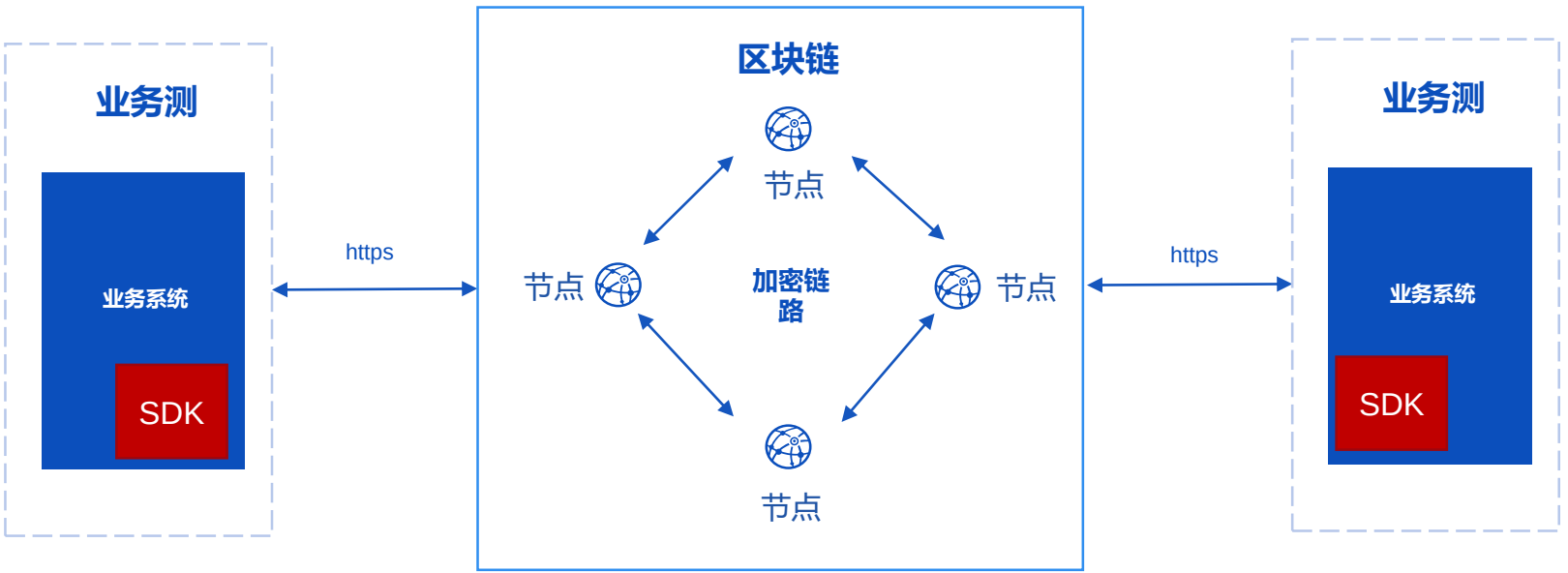
一体两翼多引擎

区块链业务开发全流程


02
开发
合约
Solidity合约开发
提供业务模版
01
搭建
区块链
提供快速建链工具
一键安装
03
部署
合约
交互式控制台部署
通过SDK部署
04
采用SDK
开发业务
JavaSDK/NodejsSDK
RPC协议交互
05
发起交易
部署业务系统
发起查询/上链交易请求

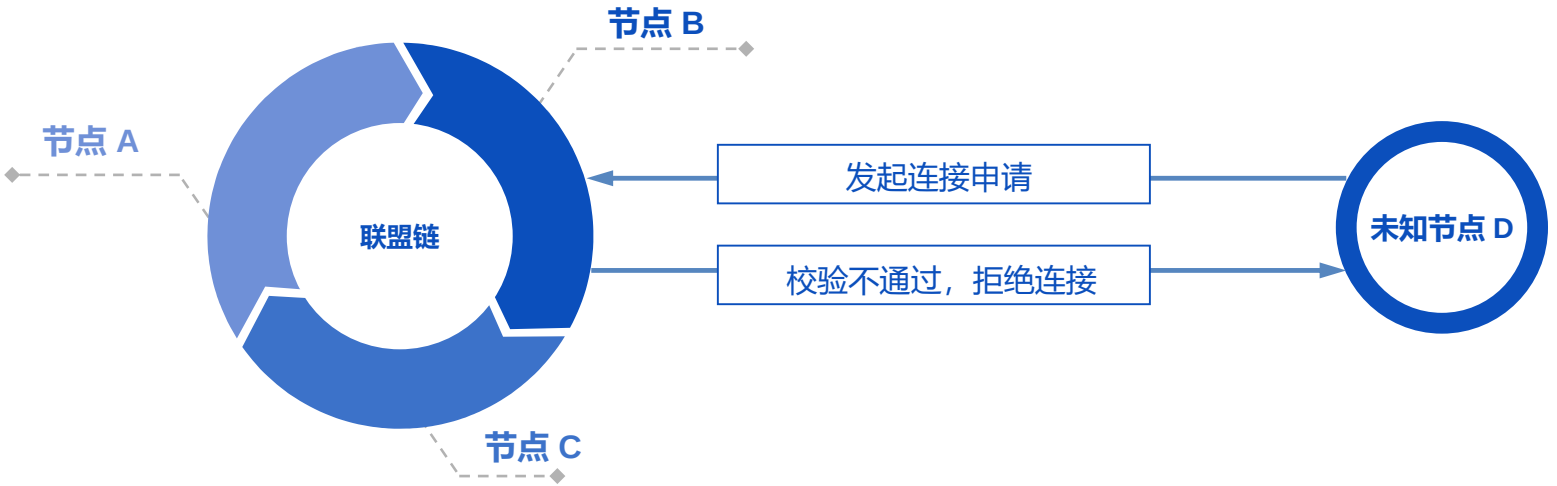
FISCO BCOS 部署架构

- 区块链可灵活选择在公有云/金融云，或者机构自有机房等的多种部署方式
- 尽可能部署在高质量网络，比如同一个云环境，或者与云环境建立高速通道



节点准入控制

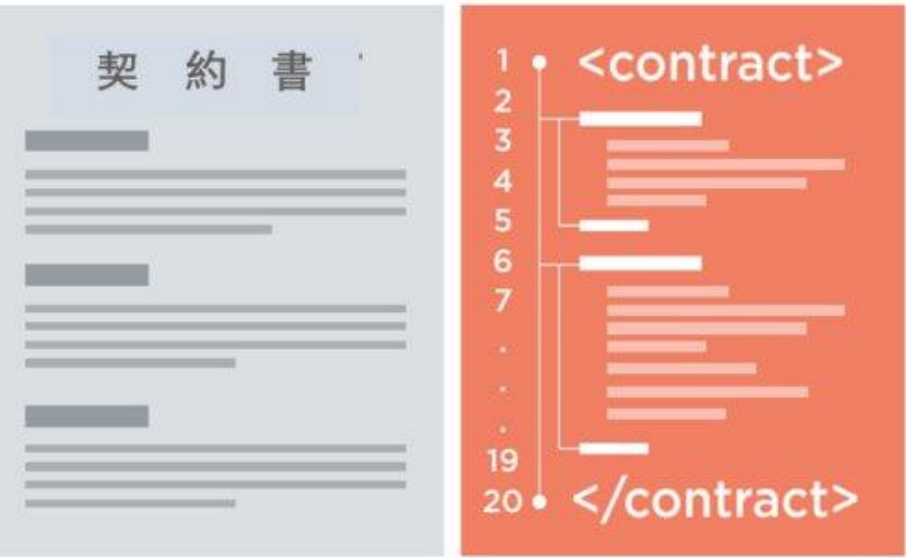
- 联盟链又称许可链，参与区块链网络的节点都需要经过准入控制
- 采用SSL通信机制，基于PKI的CA认证机制
- 节点白名单机制
- 证书黑名单机制



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

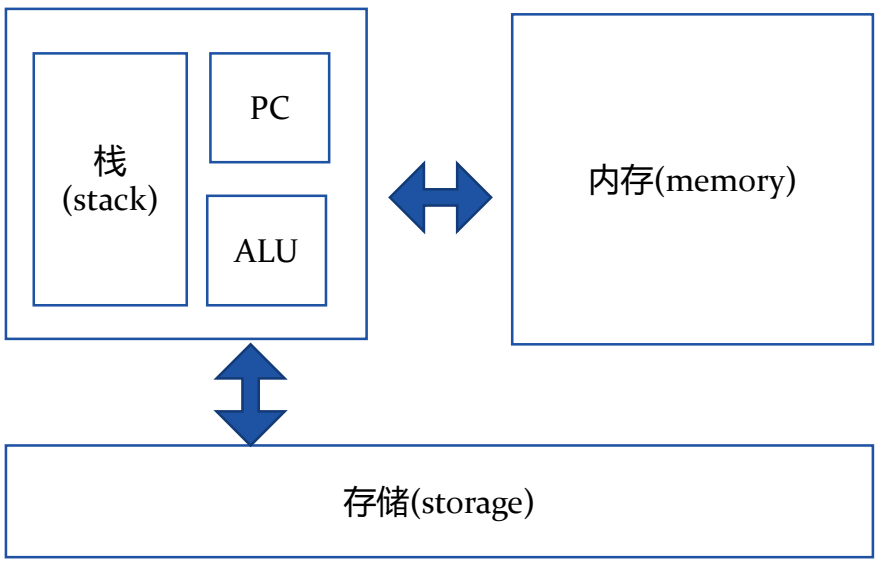
* 资产管理，合约交易，条件支付，DVP



EVM架构

EVM的核心是大小为256bit的寄存器，称为PC，PC总是指向某条EVM指令，从EVM启动开始，直到EVM停机，ALU一直不停地执行PC指向的指令，再更新PC指向下一条指令

- **栈**中每个元素的大小为256bit，栈的最大深度为1024



- **内存**是临时存储设备，在ALU执行时，用来存放智能合约和智能合约处理的数据。
- 内存是一个线性的整数数组，每个整数有唯一的地址（数组索引），大小为256bit。

- **存储**：账户拥有持久的存储空间。
- 存储是key-value结构，key和value均为256bit的二进制串，在不借助外力的情况下，存储是不可遍历的，智能合约只能读写本账户的存储，无法读写其它账户的存储

Solidity

- Solidity是运行在EVM上，面向合约的高级编程语言，它的语法受C++、Python和JavaScript的影响
- Solidity使用静态类型，支持继承、库和用户自定义类型等特性

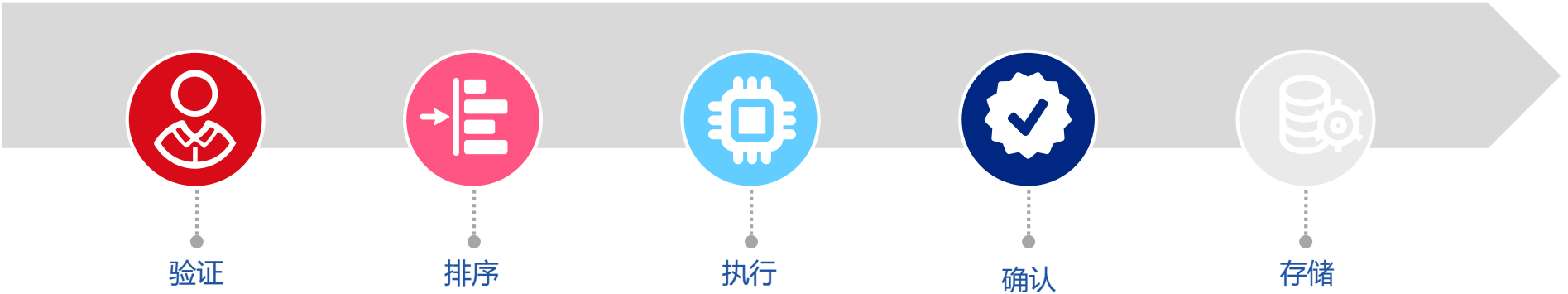
参考：http://solidity.readthedocs.io/en/v0.4.24/

区块链的速度瓶颈

一致性

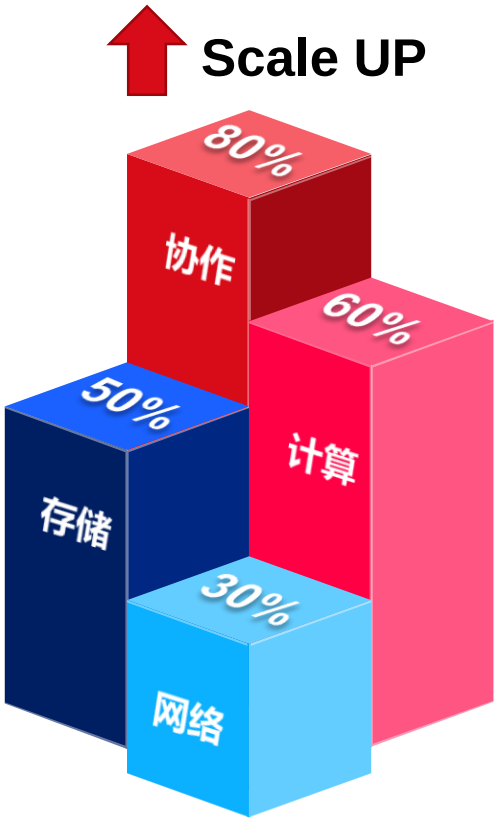
事务性

安全性



(复杂的计算开销+串行的执行模式)= （速度不高+可信安全）

性能优化之道：修炼内功



网络

优化网络互联，减少冗余流量，加速关键信息传递，处理网络抖动问题

存储

选择读写速度更快的存储方案，优化流程减少读写冲突，批量读写，适当应用缓存，减少不必要数据存储

计算

采用更高性能的库和算法，避免重复计算，无锁计算，队列化和多线程计算，更快的虚拟机,硬件计算

协作

采用高速低耗能共识算法，优化共识算法流程，协同多个节点并行验证和计算,独立事务交易并行处理，异步验证

性能优化之道：用架构的思路解决性能问题

平行扩展

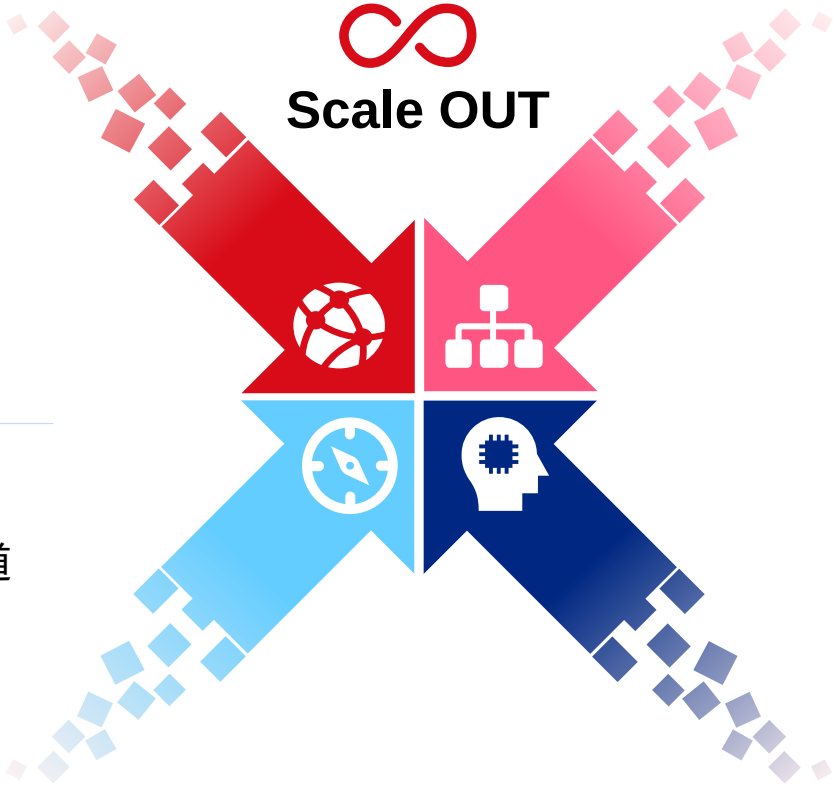
分层，多链, 跨链，通道

解决规模化和并发问题

状态通道

建立链外高速的支付通道
链上清结算

解决并发和延时问题



跨链交互

路由，中继，锚定

解决信息和资产交换问题

链外计算

在链外执行密集计算
处理大容量数据

解决计算能力和容量问题

运维友好和高可用

02

思考

1. 区块链将**颠覆**一切?

2. 区块链是一场**骗局**?

3. 智能合约真的很**智能**?

4. Code is **Law**?

5. 区块链是**可信**的?

6. 区块链是**不可篡改的**的?

7. 区块链能实现**真正的去中心化**?

WeBank

谢谢！