WeBank

FISCO BCOS 高级话题

2019年7月

FISCO 金链盟

目录

01

性能现状

性能表现的挑战

- 同时处理的交易数
- 每秒可处理交易数

- 影响交易规模
- 最直观的性能表现
- 要求越高越好

- 交易确认时间
- 交易的确定性

- 影响用户体验和业务可行性
- 要求在最短的时间内确认

- 节点数量
- 网络结构和地域

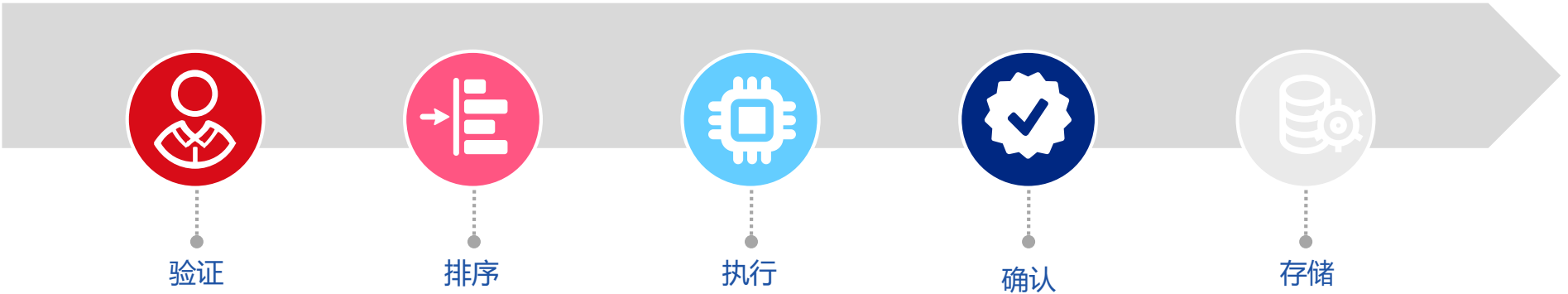
- 影响参与者数量
- 复杂网络模型的支持
- 可支持的规模越大越好

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）

区块链性能现状

- **比特币 (区块容量限制)**
  - 每10分钟一个区块，每个区块以1M，每笔交易大小250 byte来算，TPS=(1024 * 1024) / (250 * 10 * 60) ≈ 7
  - 存储和计算能力受制于单机，不会随着网络节点加入而增长

- **以太坊 (区块gasLimit)**
  - 每笔交易消耗gas，父区块决定下一个区块的block gasLimit，进而影响区块的交易数
  - gasLimit动态调整
  - 区块的交易数随着稳定增长，不适合剧烈抖动增长
  - 同样，存储和计算能力受制于单机，而且数据增长到一定规模，制约节点计算能力

- **FISCO-BCOS**
  - 兼容以太坊的EVM，采用的共识算法为PBFT，TPS≈10000
  - 存储和计算能力不再受制于单机，虚拟机可并行执行

案例

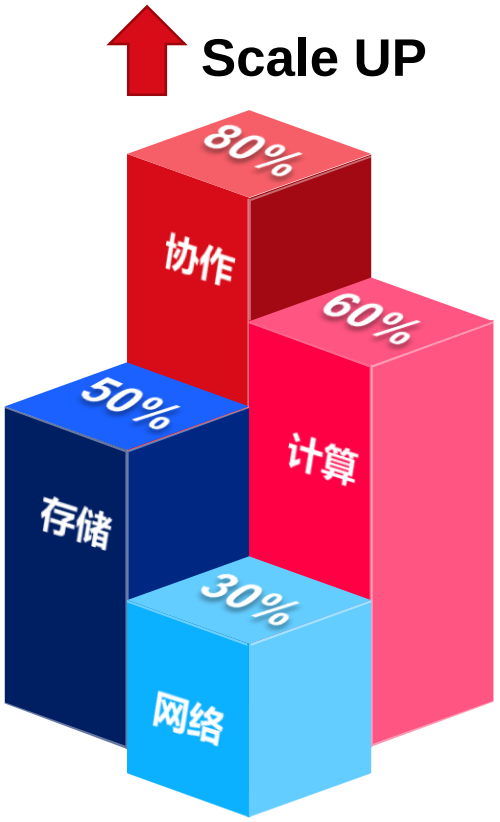
突然出现的火爆游戏--以太猫导致以太坊交易出现持续拥堵的情况，甚至某些交易在交易池中几天都处于pending状态，最终被旷工抛弃。

因此，为了解决区块链性能问题，可以从Scale Up和Scale Out两方面来引入解决方案

02

优化之道

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

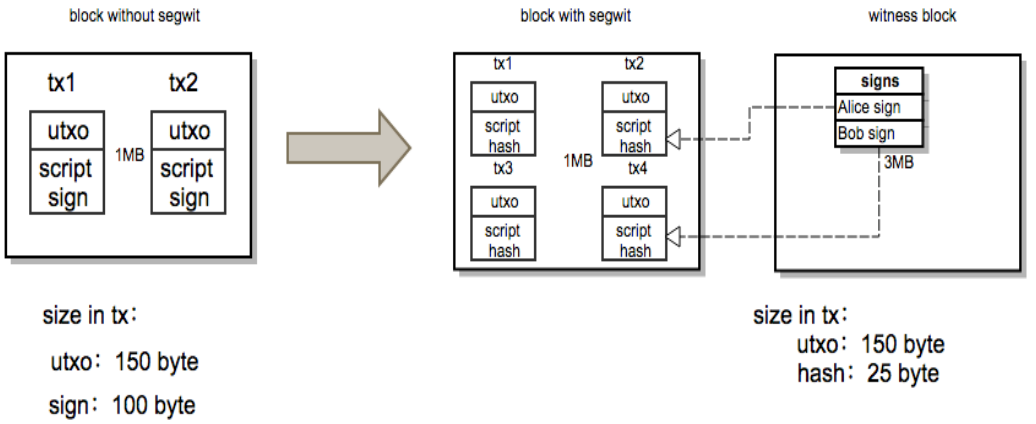
协作

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

Bitcoin优化之道

比特币：（隔离见证）

- 交易分为两大部分：utxo和脚本签名，假设大小为150字节和100字节
- 隔离见证后，区块大小依然为1M,另外带有见证witness块，见证块只有矿工才是需要的，一般的全节点和轻节点不需要
- 交易大小缩小后，区块能容纳更多的交易，借助于p2sh（pay to script hash），旧节点也可以容纳新协议的区块，软分叉



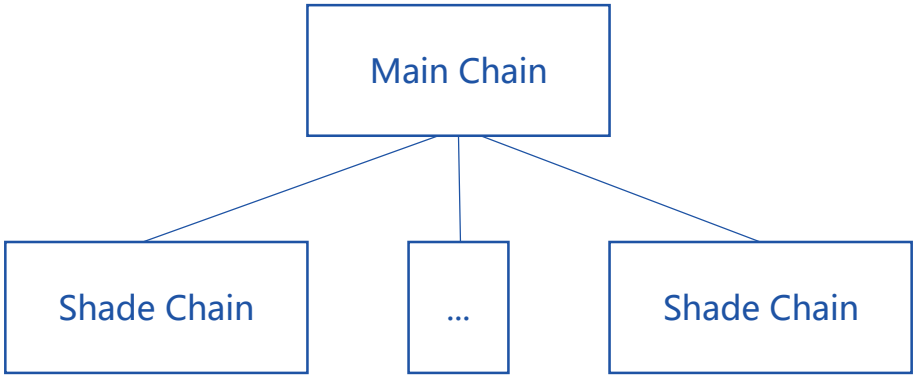
比特币：（区块扩容）

- 譬如比特现金BCH，把BTC的区块容量1M不断升级到4M->8M->32M，甚至更大区块，单纯从容量上计算，可以容纳更多的交易，进而提高TPS

Ethereum的优化之道（1/3）

以太坊：（Shading，Pos）

- 二次方分片&状态分片，在每个分组，有自己的独立状态，处理分组的交易
- POS，由Pow->Pos，不用通过解决数学难题来出块，由权益拥有者轮流或随机出块，避免了旷工竞争出块的 问题，理论上可以把块间隔时间缩短，进而提高TPS
- Validator Manager Contract，校验器管理合约，通过主链来管理分组信息

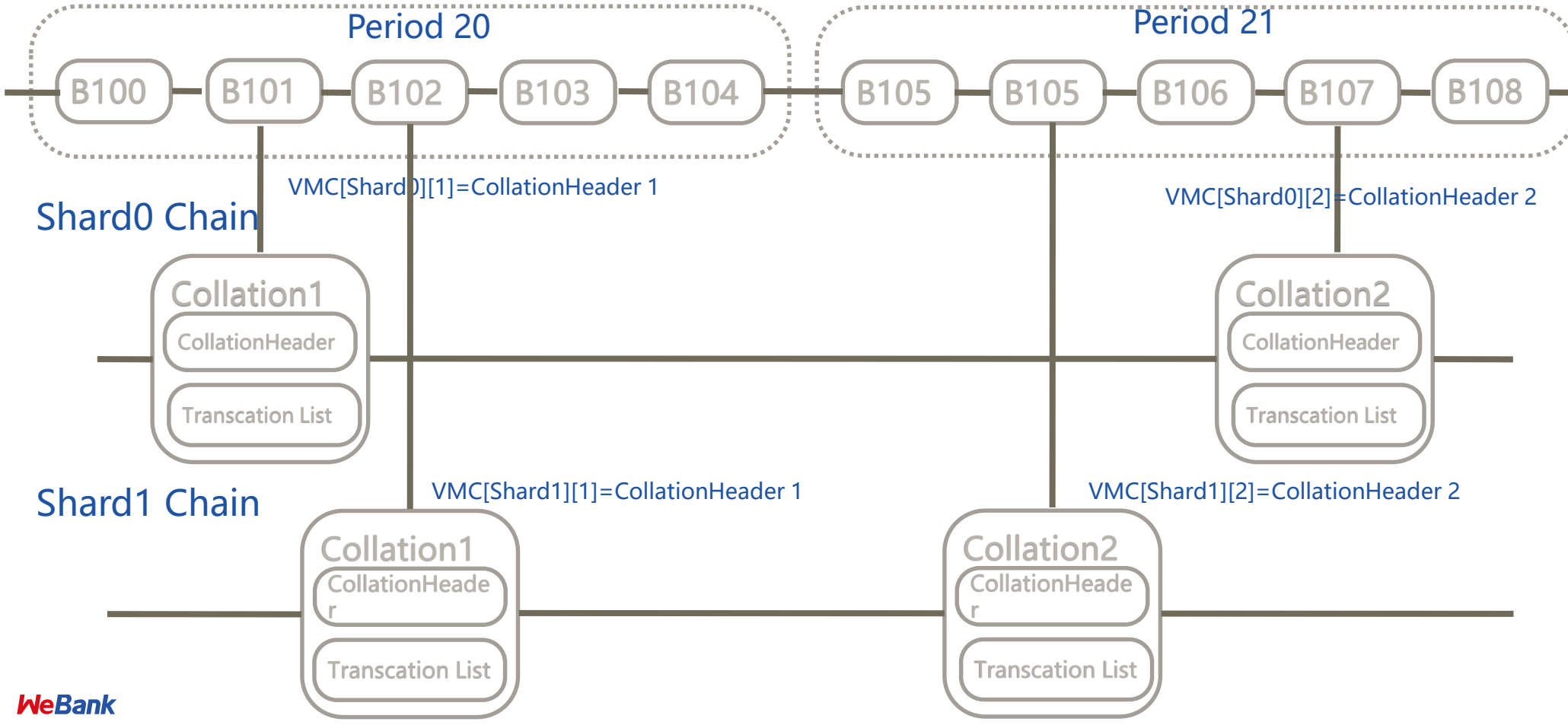


Ethereum的优化之道（2/3）

主链和分组链的交易结构

Main Chain	Shard Chain
Block	Collation
BlockHeader	CollationHeader
Miner	Callator

Ethereum的优化之道（3/3）



性能优化之道：用架构的思路解决性能问题

平行扩展

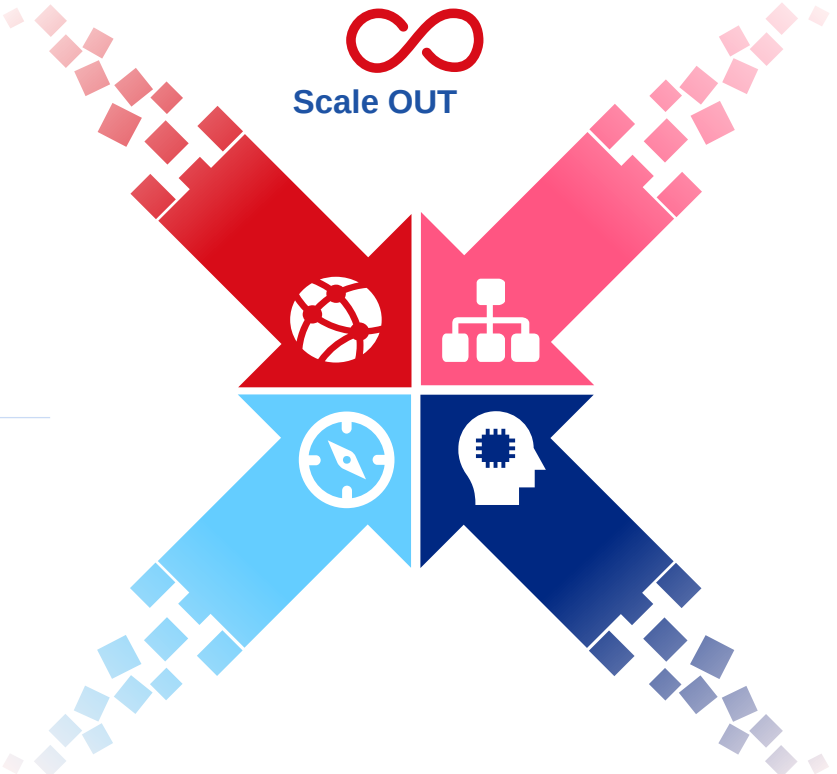
分层，多链，跨链，通道

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

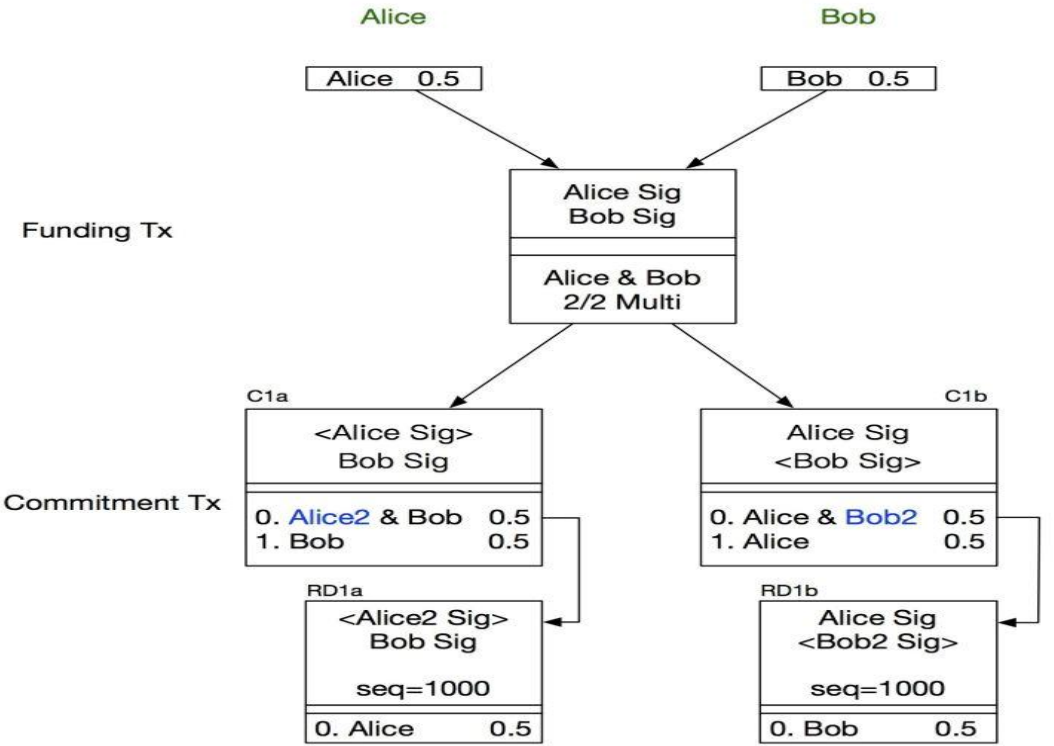
在链外执行密集计算
处理大容量数据

解决计算能力和容量问题

Bitcoin优化之路--闪电网络(小额支付)

RSMC--序列到期可撤销合约

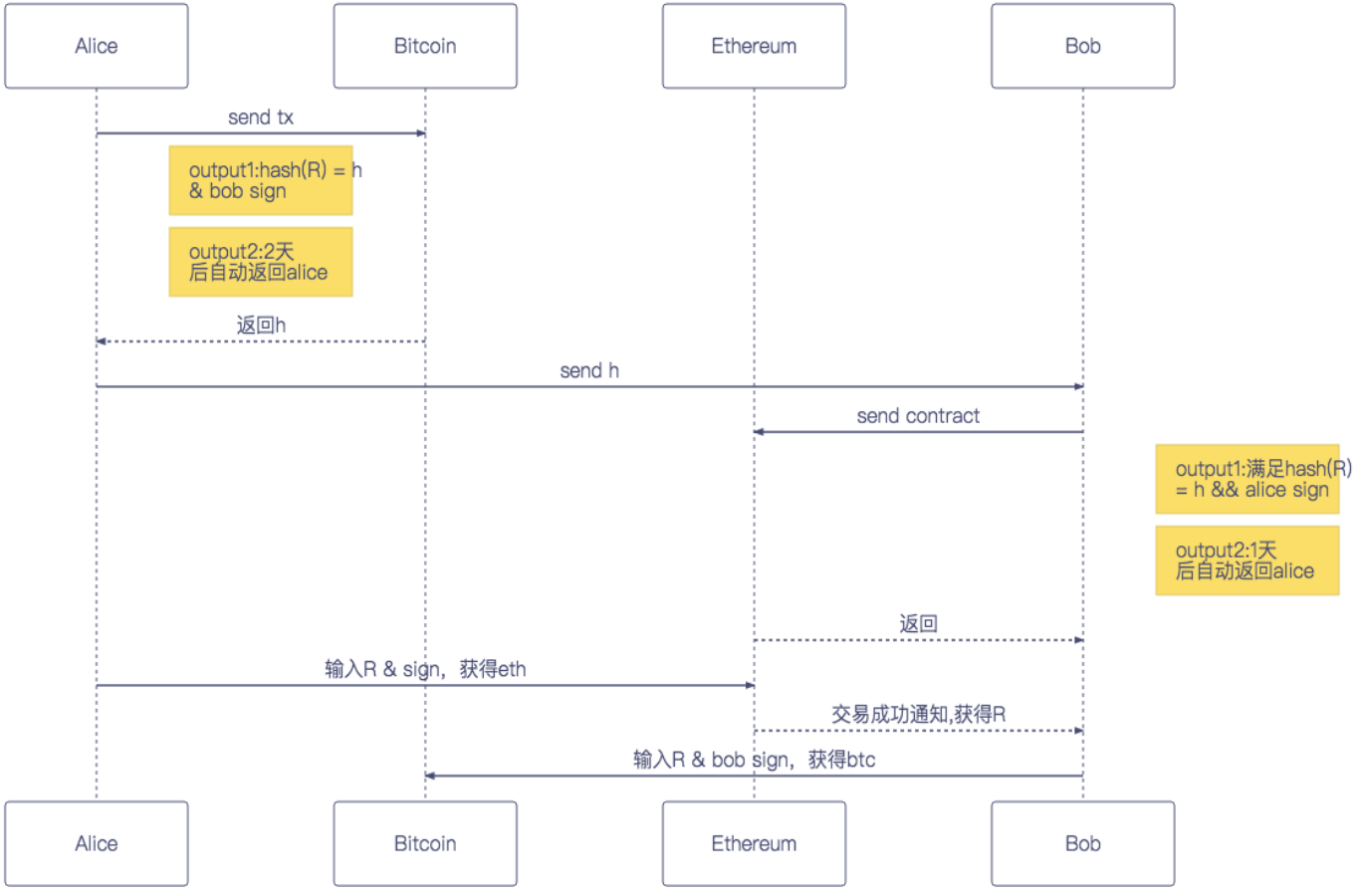
- 双方各拿出若干BTC构建tx，输出为双方的多重签名
- A构造承诺commitment：C1a和RD1a。C1a的输入为tx的输出。最后交给B签名
- C1a的第一个输出为多重签名地址，也就是RD1a的输入，RD1a的输出为A
- 同理，B构造承诺commitment：C1b和RD1b。C1b的输入为tx的输出。最后交给A签名
- C1b的第一个输出为多重签名地址，也就是RD1b的输入，RD1b的输出为B
- 各自对tx进行签名



闪电网络HTLC--Hash Time Lock Contract

HTLC--哈希锁定

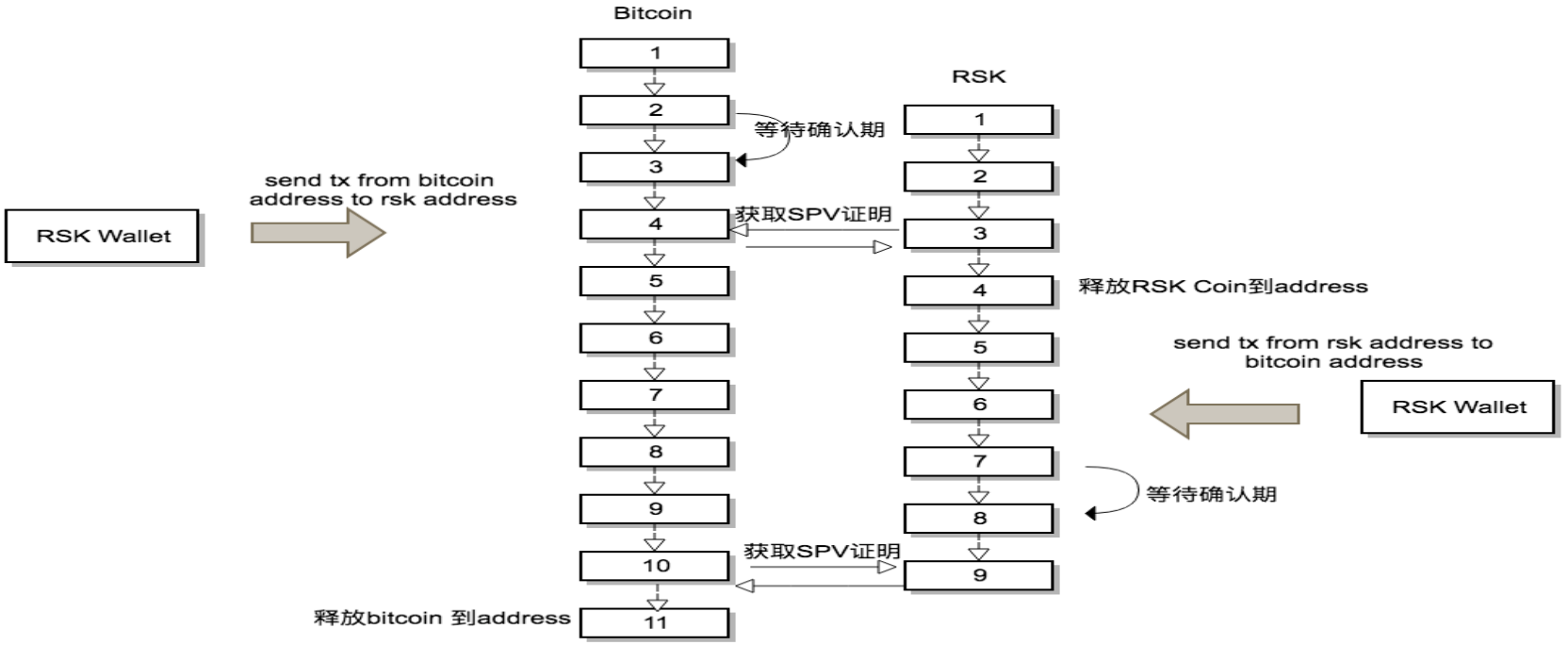
- Alice通过btc换取eth，Bob通过eth换取btc
- Alice创建一个脚本输出，只要满足两个条件之一，即可得到Alice的btc
- Alice发送hash(r)给Bob，Bob在以太坊发布合约，只要满足两个条件之一，即可得到Bob的eth
- 如果交易过程中超时，则各自的coin按原路规定时间返回



Bitcoin优化之路--侧链RSK(解决比特币TPS)

与比特币双向锚定，RSK资产来源于比特币，自身并没有创造资产。其特点是可扩展TPS，确认速度快

锚定过程采用了门限签名来保障资产的安全；与比特币联合挖矿

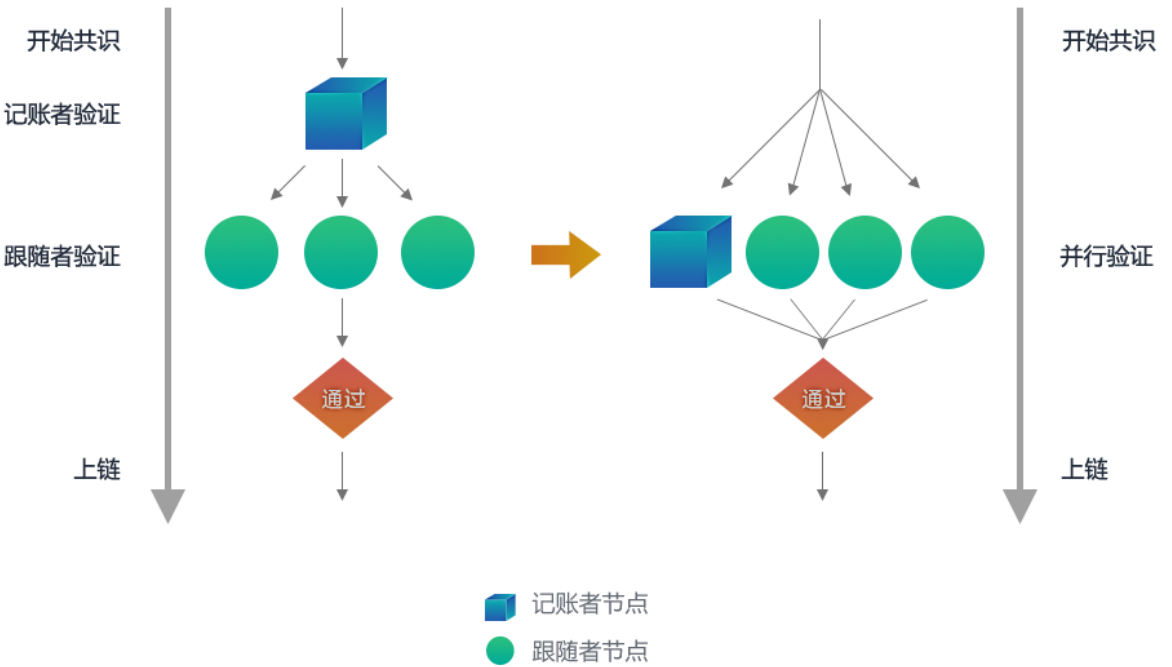


03

FISCO BCOS 演化之道

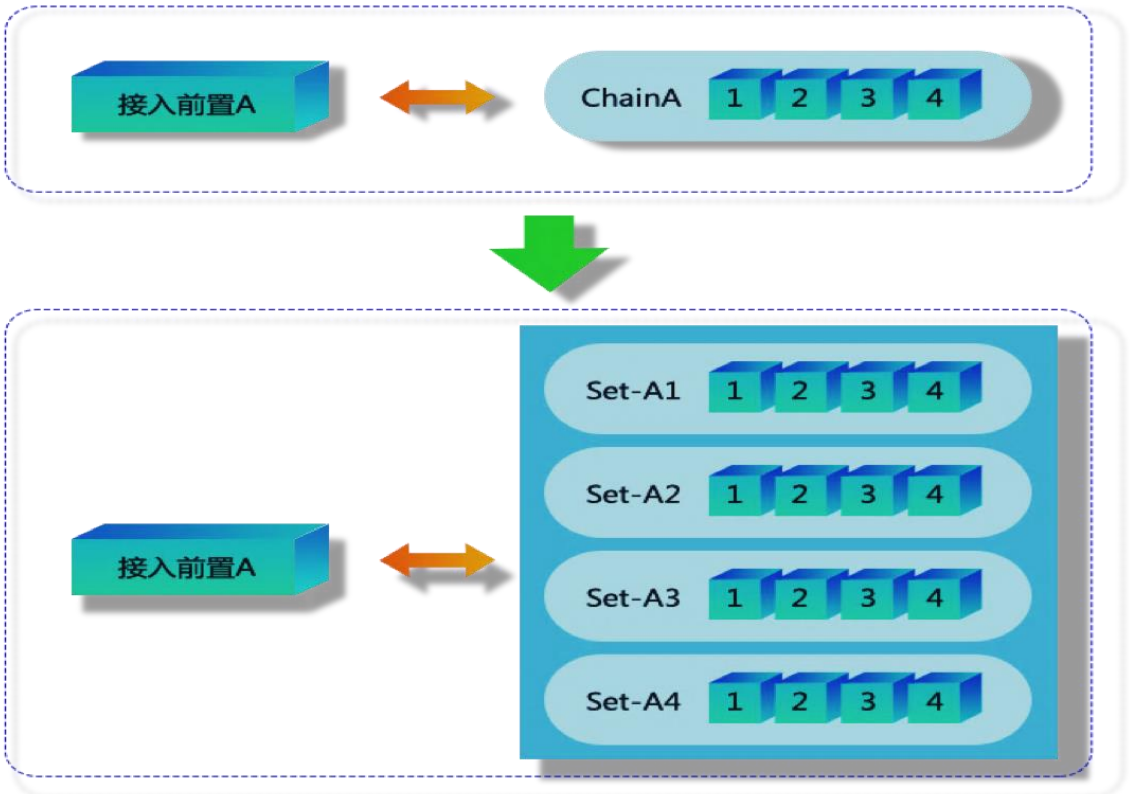
高效并行共识

- 记账者与跟随者同时并行计算，大幅提升交易处理速度
- 提升响应速度：综合评估交易计算时间和共识协商时间，在尽量短的共识周期内处理更多的交易
- 不出空块，减少存储量，加快同步速度
- 加速记账节点的互相检测，异常时可快速切换到下一个记账者。



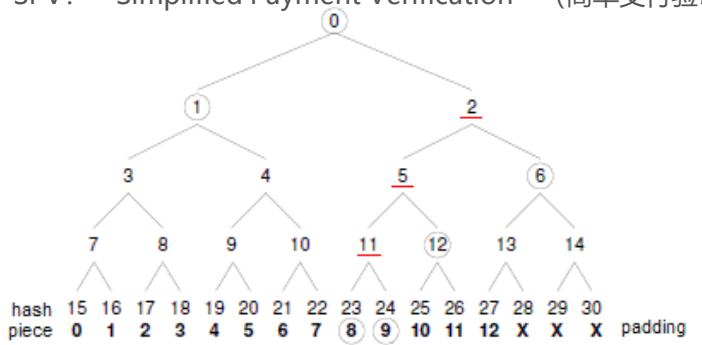
多链并行架构和跨链

- 多链并行架构，可动态扩容，支持海量服务
- 可按用户数自动分配路由策略
- 交易确认时生成通知事件，通过链上链下通道通知业务层，或向其他链发起跨链请求



一种跨链通信原理：让链A和B互相信任

* SPV： “Simplified Payment Verification” （简单支付验证）



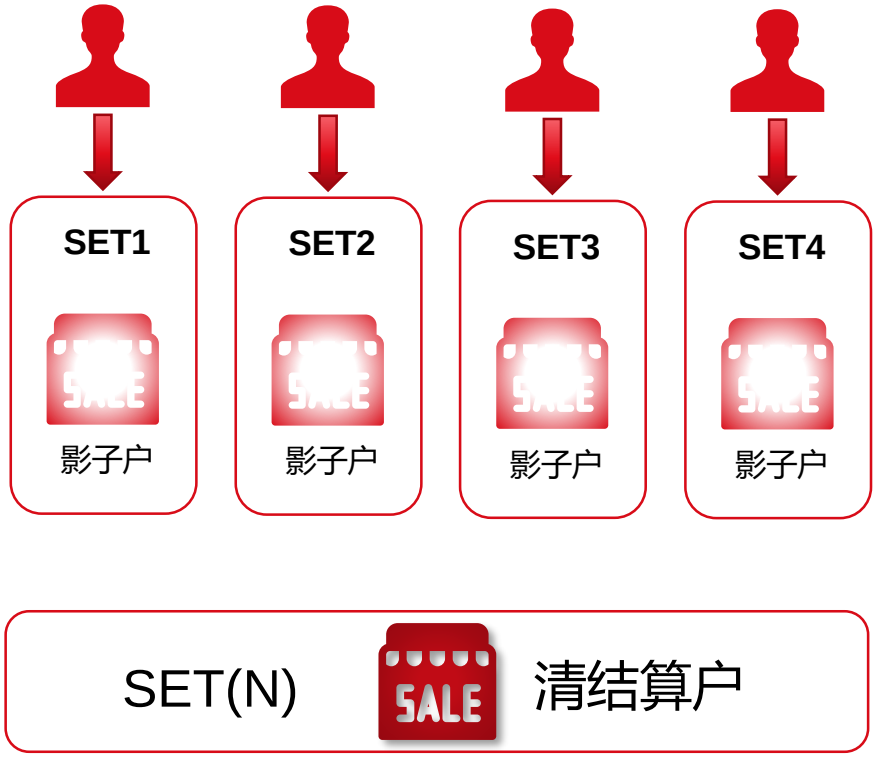
交易数量	区块近似大小	路径大小(Hash数量)	路径大小（字节）	路径和区块比
16	4KB	4	128	3%
512	128KB	9	288	2.1%
2048	512KB	11	**352**	**0.06%**
65535	16MB	16	**512**	**0.0025%**

* 以上数据仅供参考

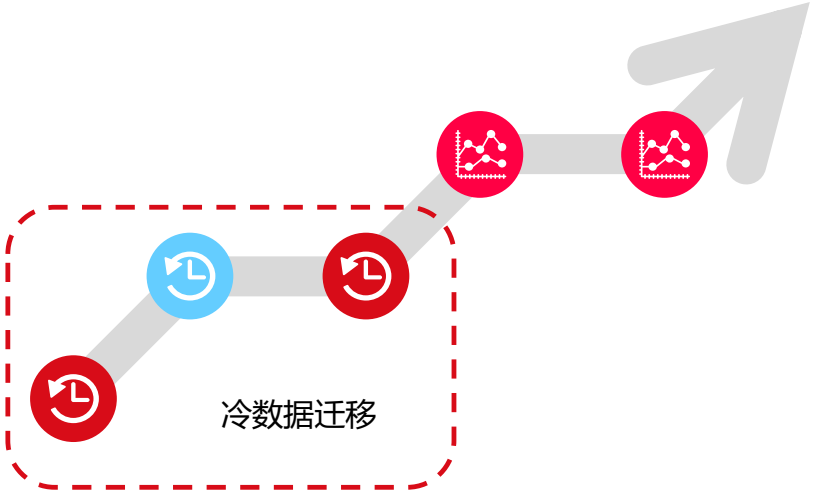
典型金融场景：热点账户问题解决

并发的海量用户向同一个商户帐户发起交易，在集中处理的情况下，该商户会成为热点帐户，处理缓慢

将实时交易分解到不同的SET里，并行处理用户交易。异步发起账目归集和进行清结算

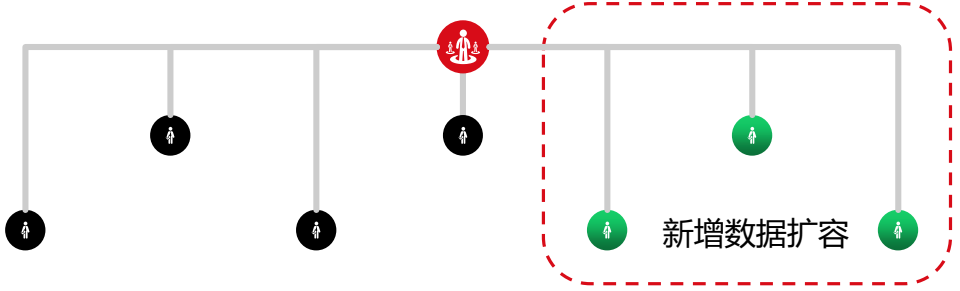


数据扩容和迁移



➢ 数据裁减：

- 如数据有较强的时间属性，可对冷数据进行裁减
- 根据区块高度打标签，把旧交易数据迁移到数据仓库
- 状态数据保留快照，历史数据迁移到数据仓库
- 查询旧数据时重定向到数据仓库



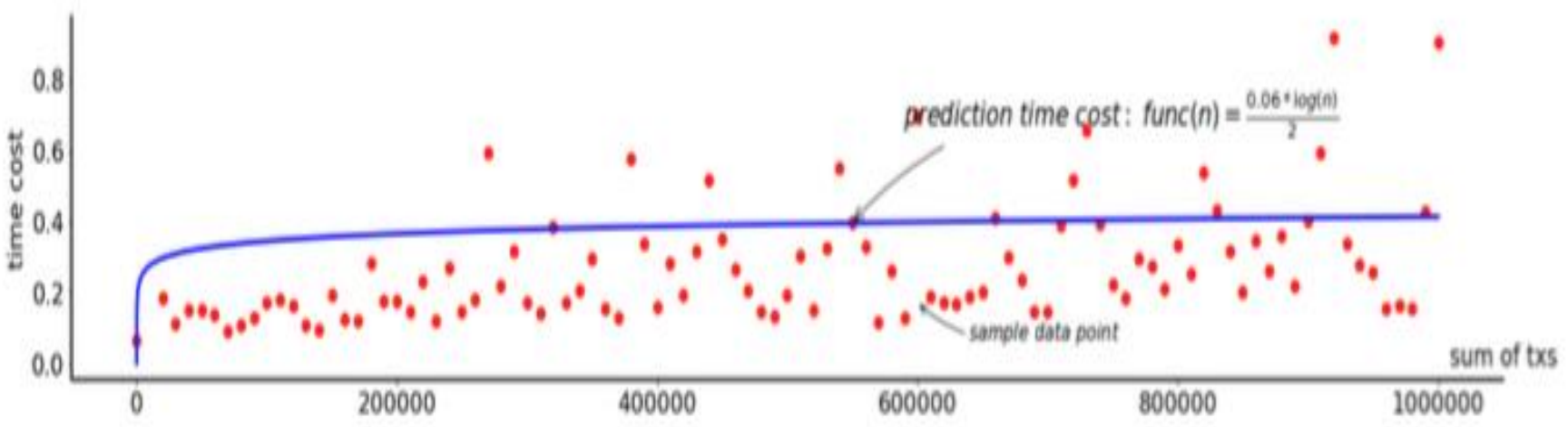
➢ 持续扩容：

- 根据帐号、业务等维度持续增长的数据可持续扩容
- 采用多链架构，加入新的硬件资源进行平行扩容
- 设计路由规则，将交易分发到不同的链上

分布式存储AMDB

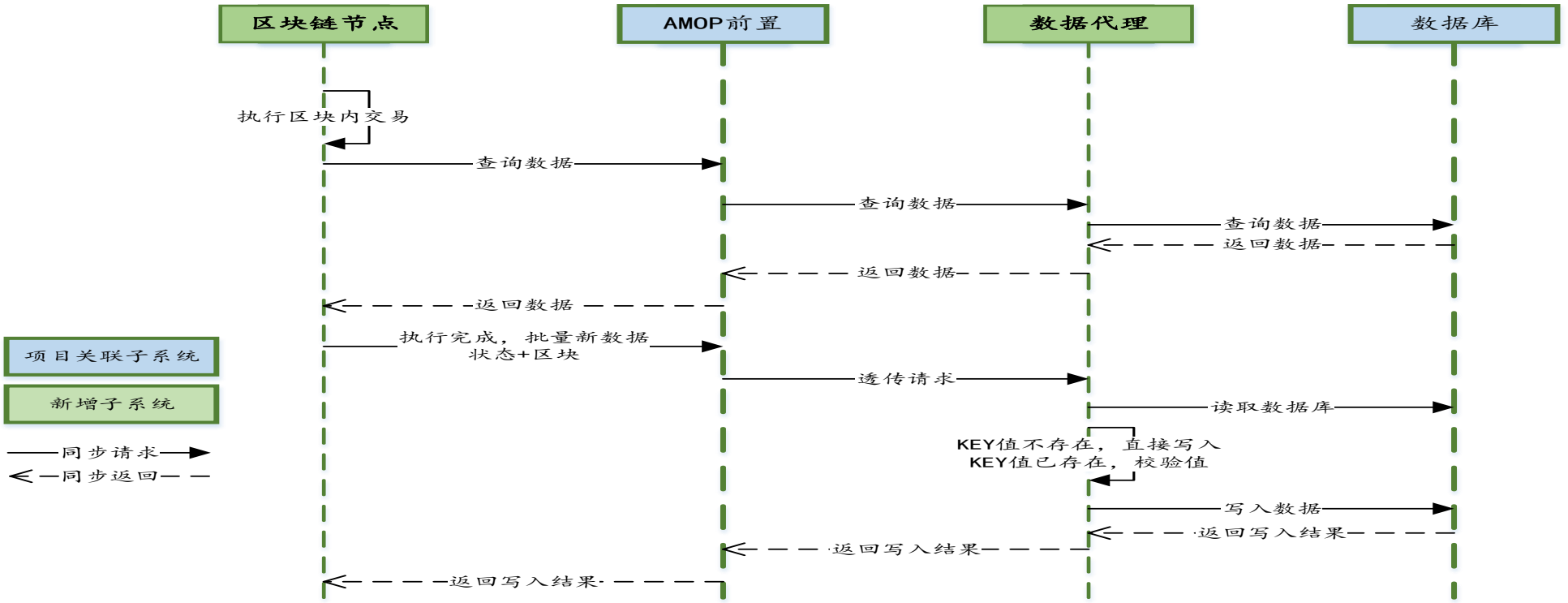
- MPT树使区块链拥有可追溯，防篡改等能力
- 随着数据量增大，复杂的结构迎来的是查询随机读写的性能瓶颈
- 在联盟链中，运用了PBFT，溯源能力并不是关键

交易量与性能（“毛刺”随之增加）



优势

- 分布式存储，数据存储不受单机容量限制
- 合约支持高级特性，转化为类SQL查询，对用户更友好
- 废弃了世界状态，采用新的存储结构，更高的TPS



04

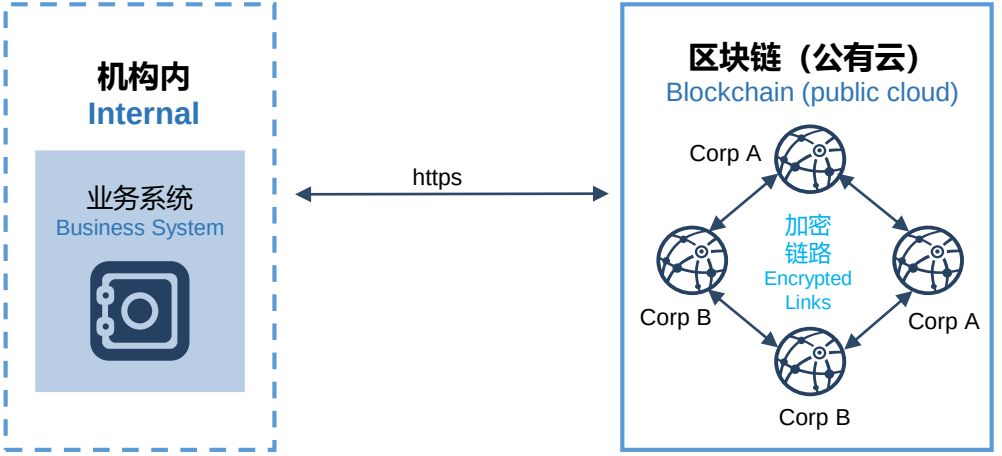
运维友好和高可用

多种编译方式

源码编译安装	一键部署	物料包	Docker	云服务
从源代码开始，进行编译安装配置运行 自由度高，适合有一定经验的开发者	通过脚本方式，一键编译， 在本机安装和运行多个节点 简单便捷，适合开发环境，快速体验	为特定操作系统准备的安装文件，无需编译，直接安装 适合无需重新定制的生产和测试环境	采用Docker方式快速安装部署，和已有Docker管理环境整合 适合已有Docker管理的环境	通过云服务平台获取区块链服务

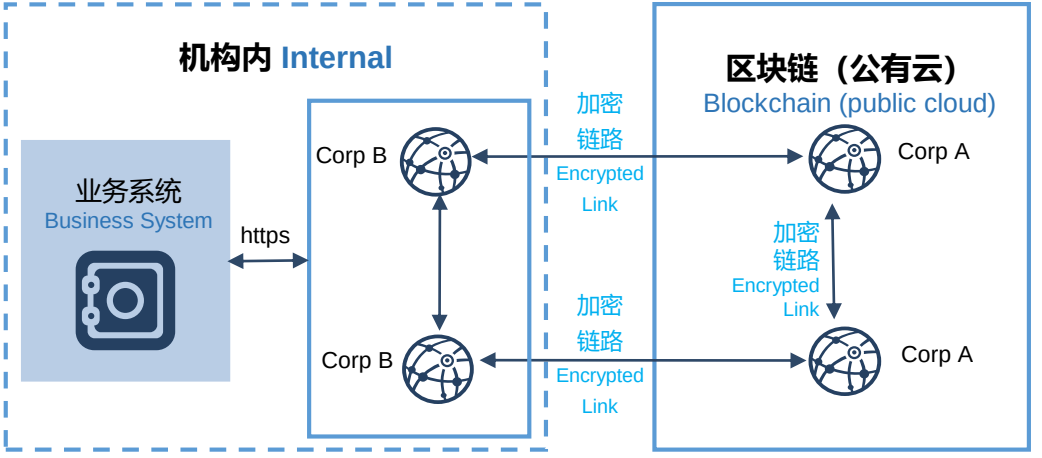
- 提供多种编译部署方式，满足学习，开发，测试，生产，云服务等多场景的需求
- 最快可1分钟建链，开启区块链深度探索之旅

适应多种环境的部署方式



公有云部署方案

Public Cloud
Deployment



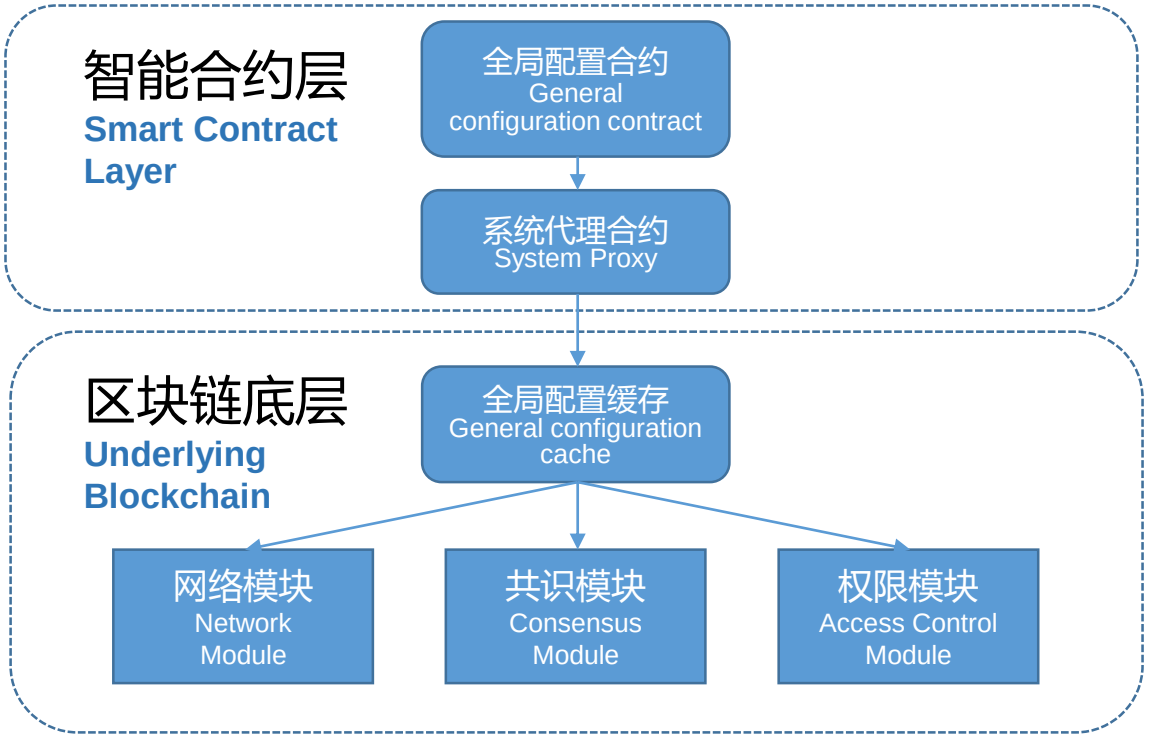
机构内部署方案

Internal
Deployment

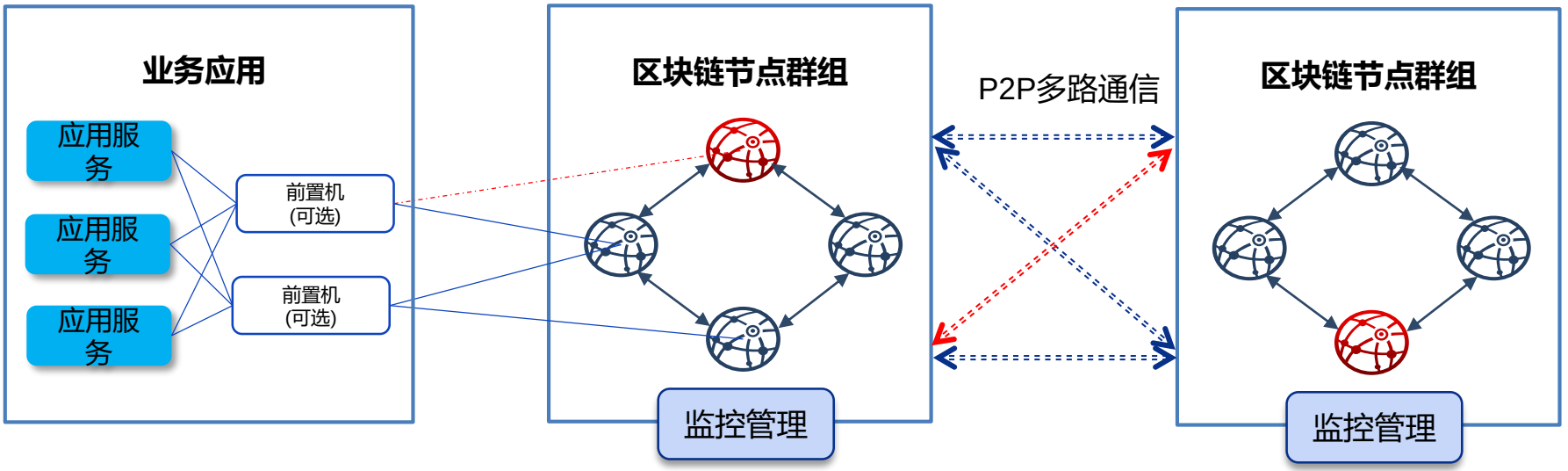
全局配置更新

- 全局配置写入系统合约，全网一致
- 通过发送交易更新配置，保证全网同步更新

- 支持动态的：
  - ✓ 调整性能
  - ✓ 加入和退出节点
  - ✓ 设定CNS
  - ✓ 设置权限
  - ✓ ...



健壮性设计



- 应用多活，同时和多个区块链节点通信
- 多区块链节点形成对等网络，支持多活服务，互相备份
- 立体监控，包括服务器监控，进程监控，区块链运行时特性监控，账目数据监控，异常告警
- 专业运维团队参与运维，定期更新版本，新版本向下兼容

构建金融级监控和高效运维体系

治理与管控能力加强，满足金融行业对数据结构化、可视化、可监管、可审计的要求

区块链浏览器

实现区块链信息的获取、统计及可视化

监控指标

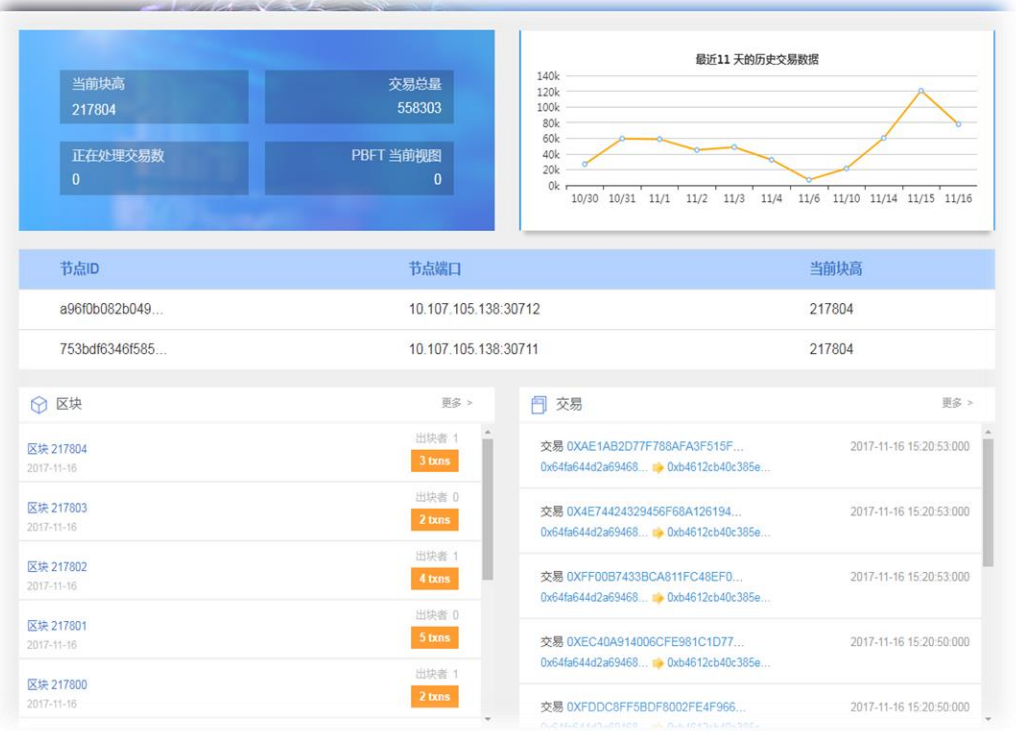
预埋关键监控指标便于精细化运营

运维部署

灵活部署，智能运维，动态扩容

治理能力

全局配置，灰度升级，版本兼容



科技创新之路

知识

- 计算机基础理论
- 数学，信息学
- 经济学,社会学
- 博弈论，概率论
- ...

技术

- 平台框架
- 编程语言
- 开发工具
- 模块设计
- 算法类库

方案

- 业务需求
- 系统架构
- 概要设计
- 详细设计
- 成本预算

实施

- 项目管理
- 团队管理
- 质量保障
- 功能性能
- 系统交付

运营

- 用户市场
- 运维监控
- 稳定可控
- 系统升级
- 容量扩容

05

应用扩展

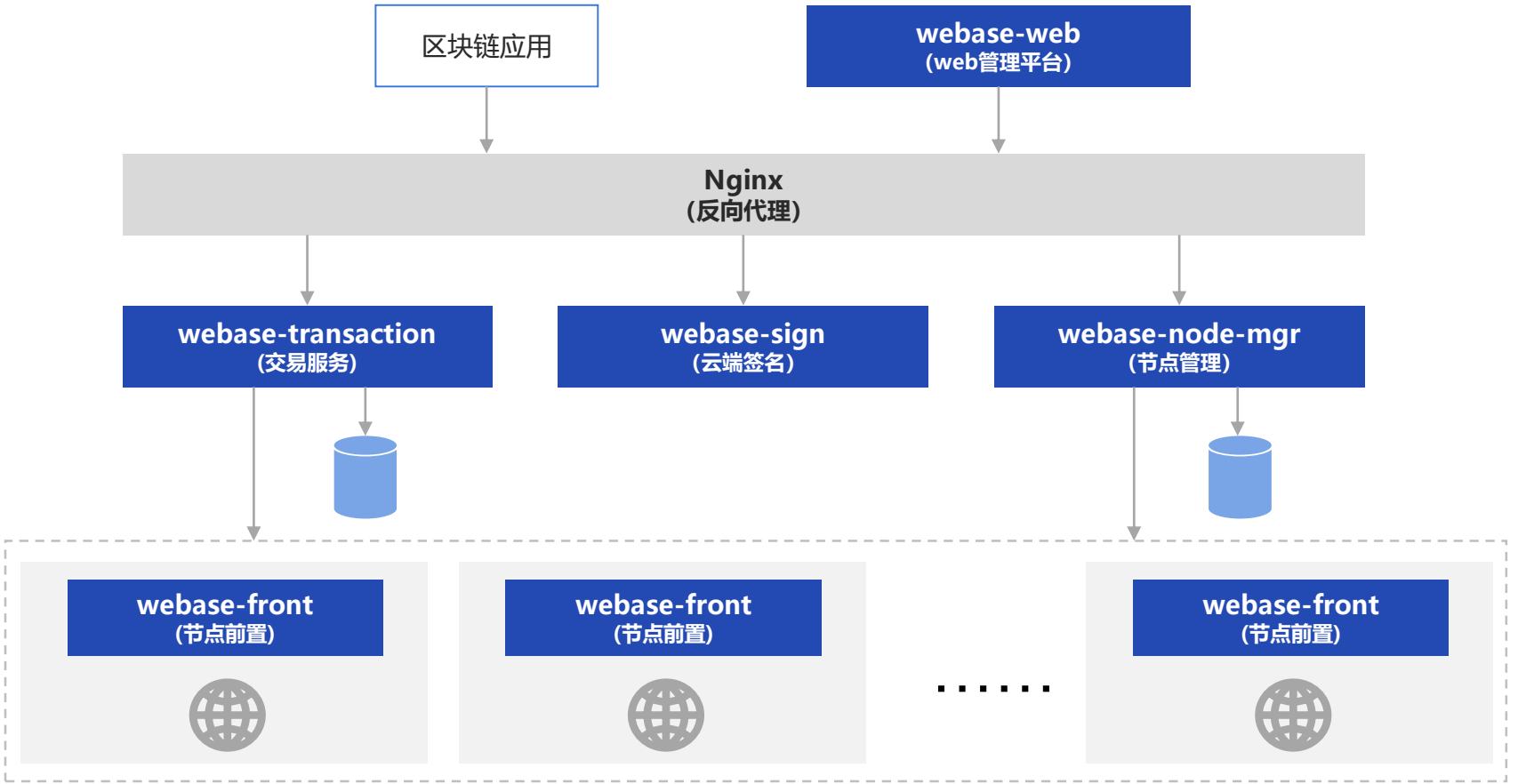
WeBASE：覆盖区块链应用全生命周期

区块链应用

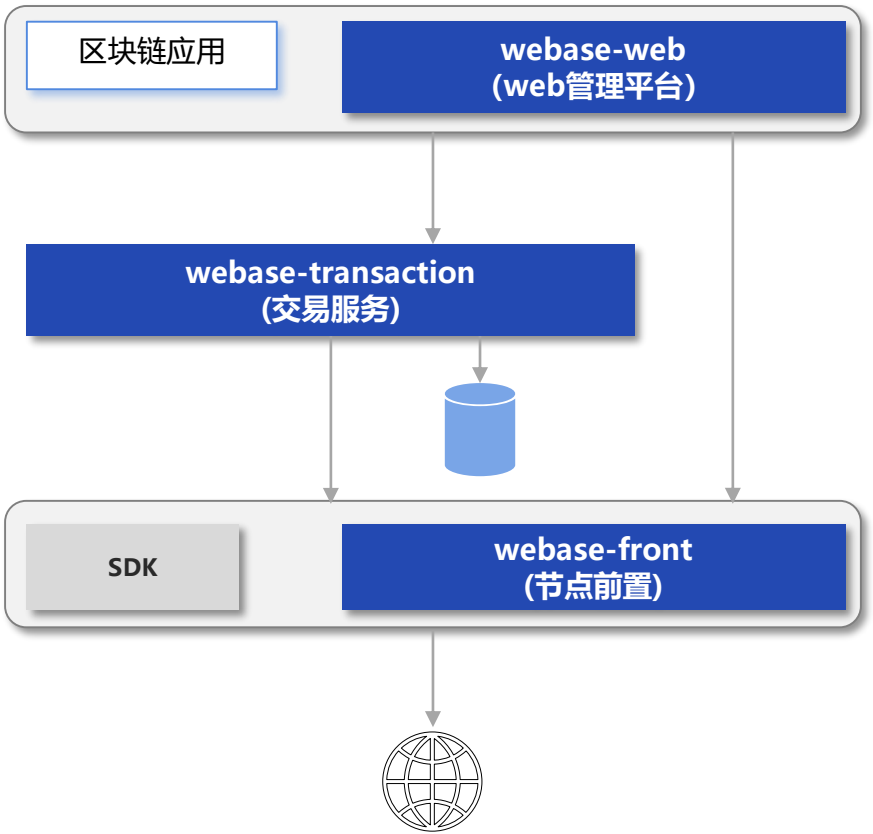
管理平台	智能合约	交易	数据
区块浏览	合约管理	交易缓存	数据导出
节点管理	合约开发IDE	异步上链	数据获取API
合约管理	合约代码托管	交易API	数据可视化查询
监控视图	本地编译	云端签名	数据分析
异常交易审计	可视化部署	私钥托管	业务监控

FISCO-BCOS底层

WeBASE：部署架构


区块链应用
webase-web
(web管理平台)
Nginx
(反向代理)
webase-transaction
(交易服务)
webase-sign
(云端签名)
webase-node-mgr
(节点管理)
webase-front
(节点前置)
webase-front
(节点前置)
webase-front
(节点前置)

WeBASE：交易上链



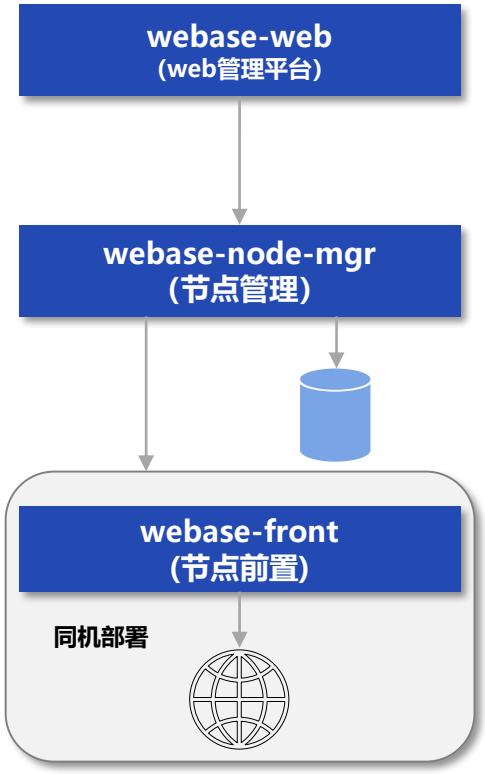
webase-transaction

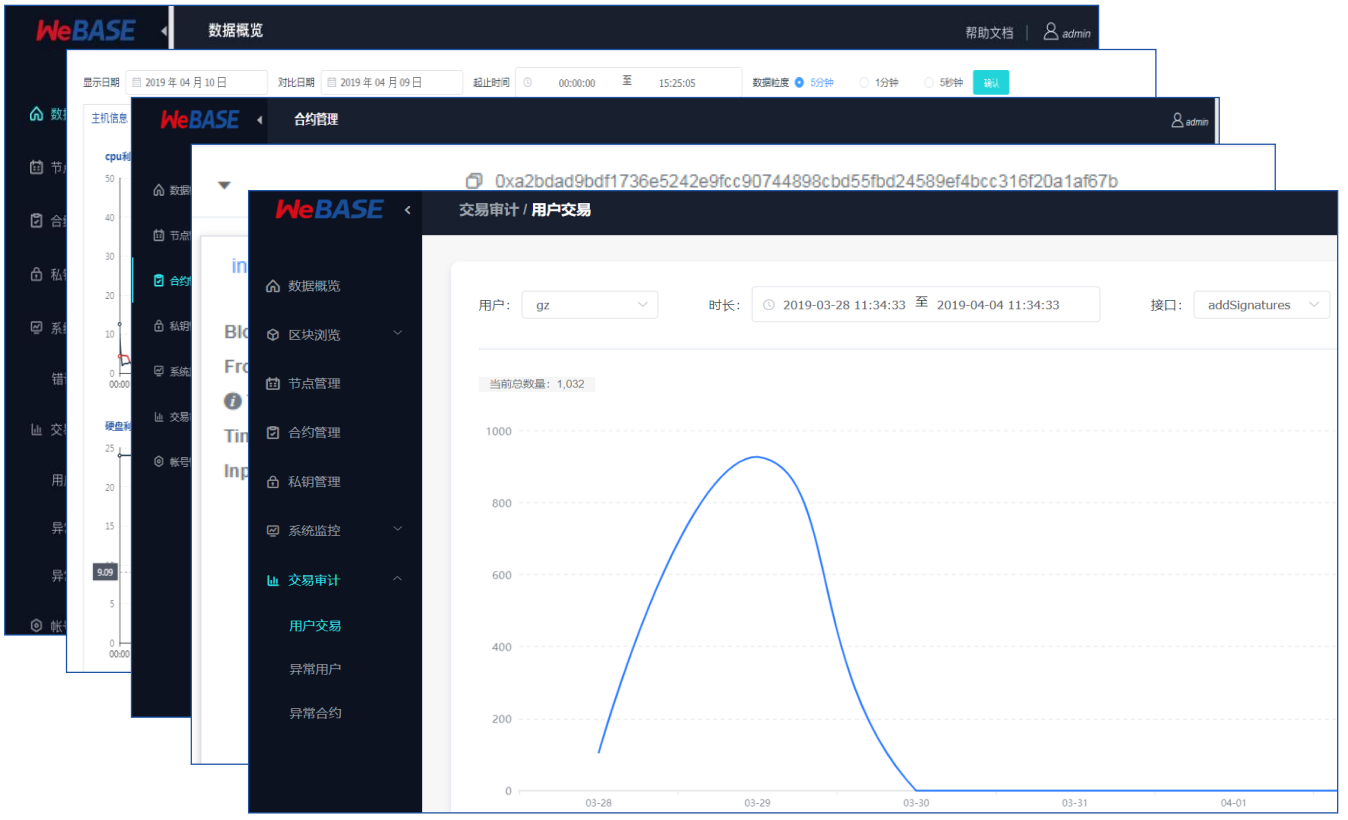
- 无需集成SDK
- 用用层支持多语言
- 交易缓存，满足高并发请求
- 异步上链
- 数据校验

webase-front

- 节点前置和节点同机部署
- 封装web3jsdk，提供restful风格接口
- 内置网页控制台
- 内助内存数据库，采集节点性能数据
- 快速上报区块数据到指定服务器

WeBASE：管理平台


webase-web
(web管理平台)
webase-node-mgr
(节点管理)
webase-front
(节点前置)
同机部署


WeBASE
数据概览
帮助文档
admin
合约管理
0xa2bdad9bdf1736e5242e9fcc90744898cbd55fbd24589ef4bcc316f20a1af67b
交易审计 / 用户交易
数据概览
区块浏览
节点管理
合约管理
私钥管理
系统监控
交易审计
用户交易
异常用户
异常合约
用户：
gz
时长：
2019-03-28 11:34:33
至
2019-04-04 11:34:33
接口：
addSignatures
当前总数量：1,032
1000
800
600
400
200
0
03-28
03-29
03-30
03-31
04-01

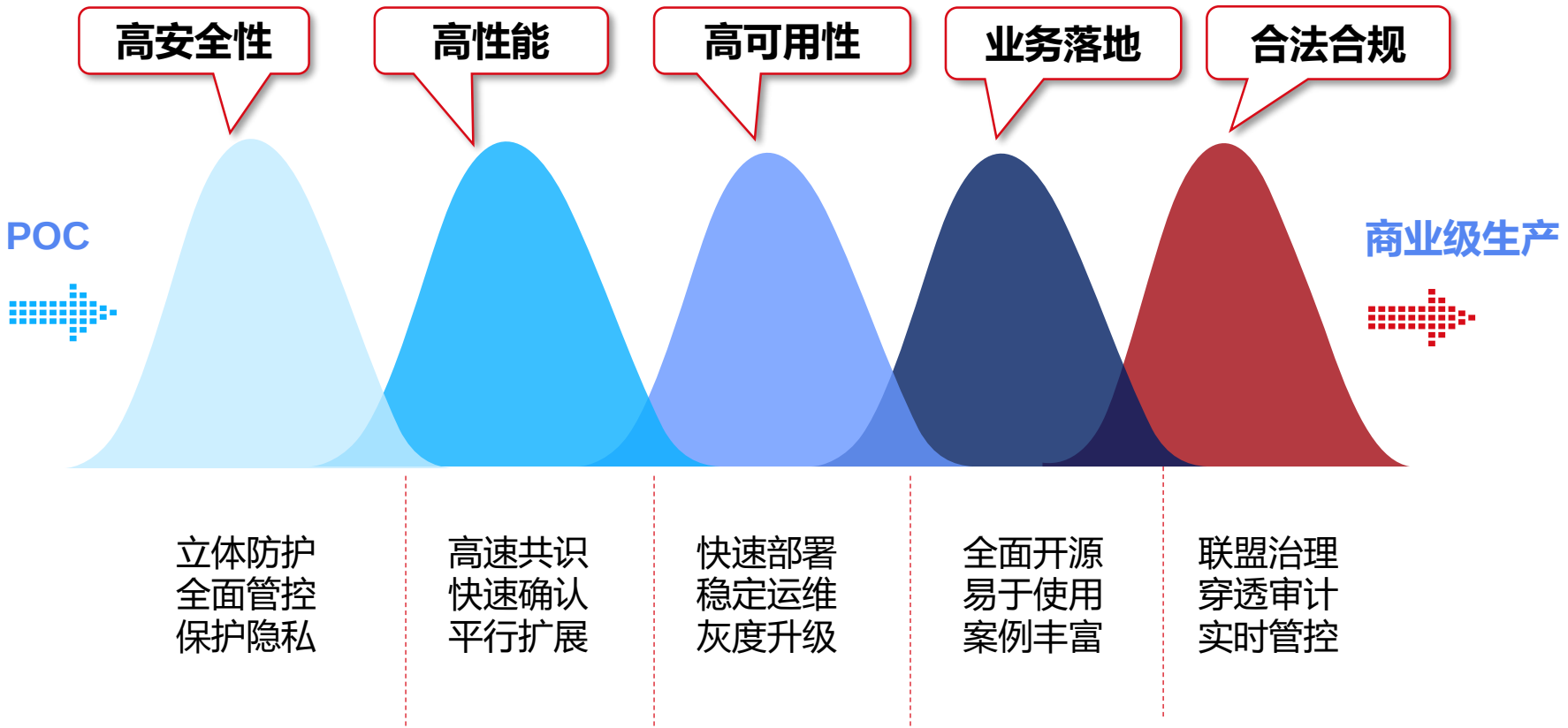
WeBASE：私钥管理和签名

- 客户端本地签名
- 云端签名
- 多种私钥存储方式供选择

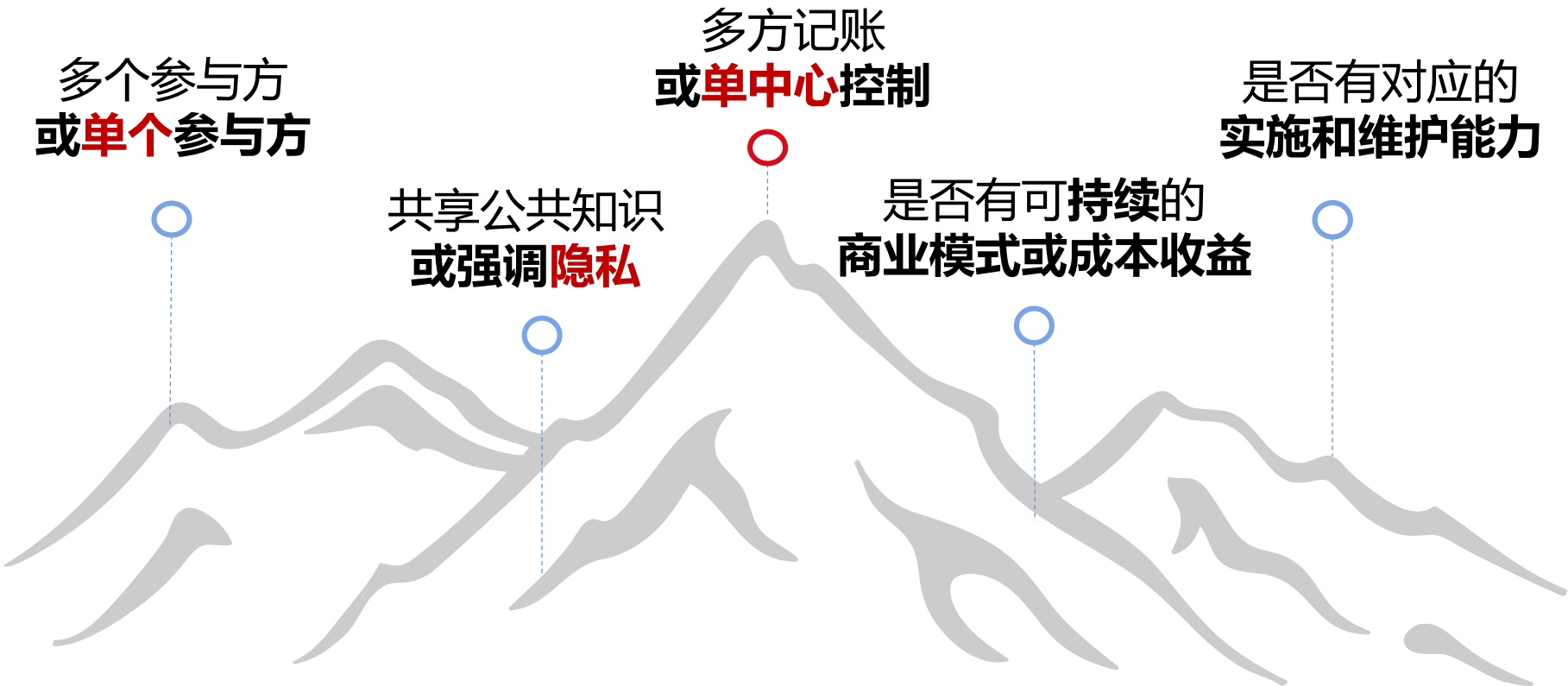
06

应用之道

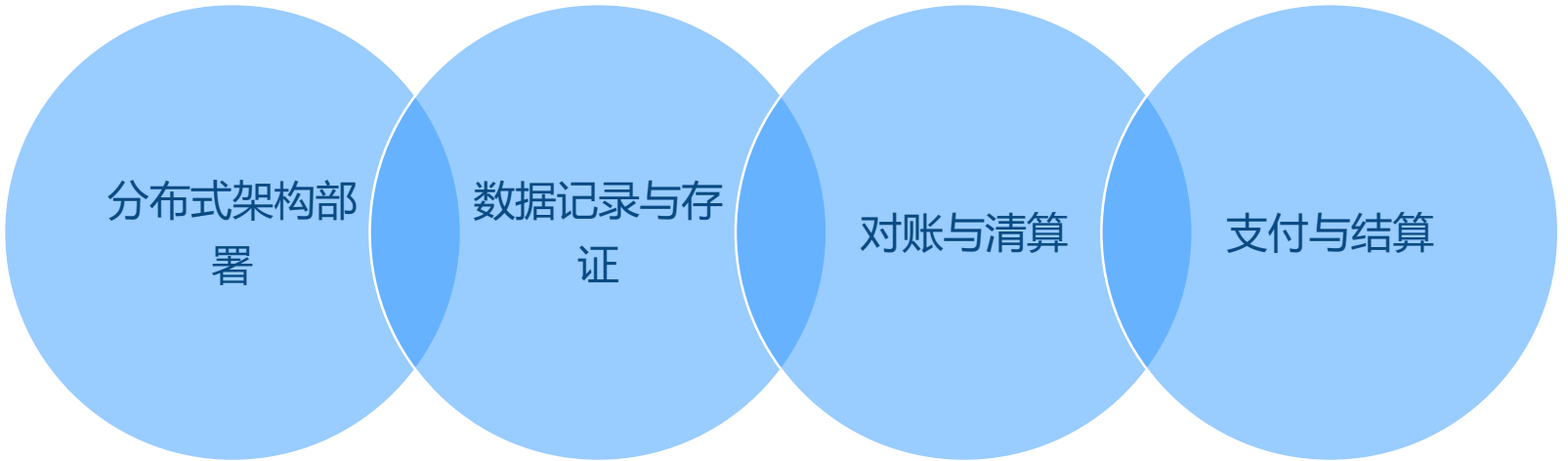
联盟链面临的挑战和应对之道



决策使用区块链的路径

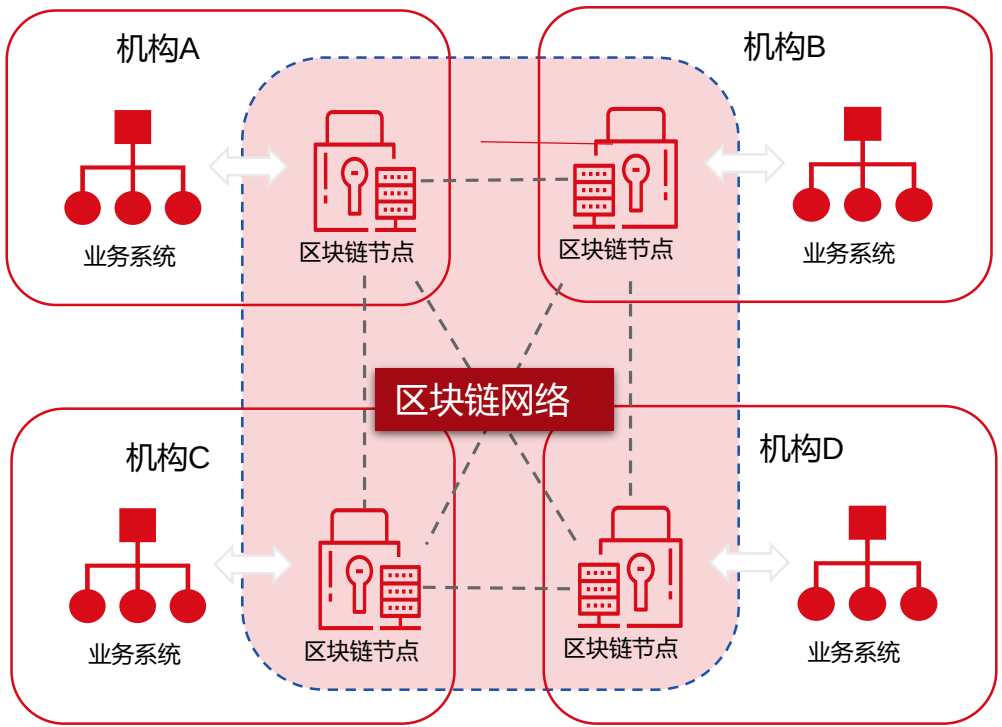

多个参与方
或单个参与方
共享公共知识
或强调隐私
多方记账
或单中心控制
是否有可持续的
商业模式或成本收益
是否有对应的
实施和维护能力

联盟链技术的主要应用



- 若应用终端的分散程度较高或负载较大，可采用分布式技术以提高健壮性或自适应性。
- 有效解决数据可信痛点，减少系统数据被篡改、被伪造或产生一致性差异的可能。
- 通过信息技术的自信任机制可解决多方的信任、协作或对等性问题；
- 基于高一致性的数据进行对账，完成账目计算
- 支持自动触发并执行智能合同、合约或条约；
- 在引入法定数字货币的前提下，可实现价值的转移。

区块链可成为机构之间创新互联的基础设施



- **跨机构边界**：打破机构间或自然人界限的分布，而不仅仅是服务器，机房，地域的分布。
- **分布式事务**：通过共识算法在交易发生时就达成一致性确定性，多家机构实时参与到交易的验证和确认中，而不是通过事后处理的方式同步。
- **博弈和信任**：在验证过程中强调抗欺诈，对抗交易者和记账者作恶。
- **冗余和可用**：计算和存储冗余，无差别计算和存储，而不是由某一个集中模块计算或有限分片计算。具有极高的容灾能力和系统可用性。
- **标准化系统**：接入一个链上的成员采用一致的软件，接口，治理方式，运维方式，可极大的降低成本提升效率

联盟链技术的主要应用领域

金融服务

支付、交易清结算、资产数字化、供应链金融、
智能证券、场外市场、票据、征信、反洗钱...

供应链管理

物品溯源、防伪、认证
物流追溯、责任认定

医疗健康

数字病历、健康管理

慈善公益

善款追溯、公益审计

文化、IP版权

专利保护、文学音乐视频游戏的版权保护
书籍许可证、艺术品证明、数字内容确权

社会管理

代理投票、身份认证、档案管理
遗产继承、公证、工商管理

教育

档案管理、学历证明、学生征信、
成绩证明、产学合作

共享经济

租车、租房、智能电网

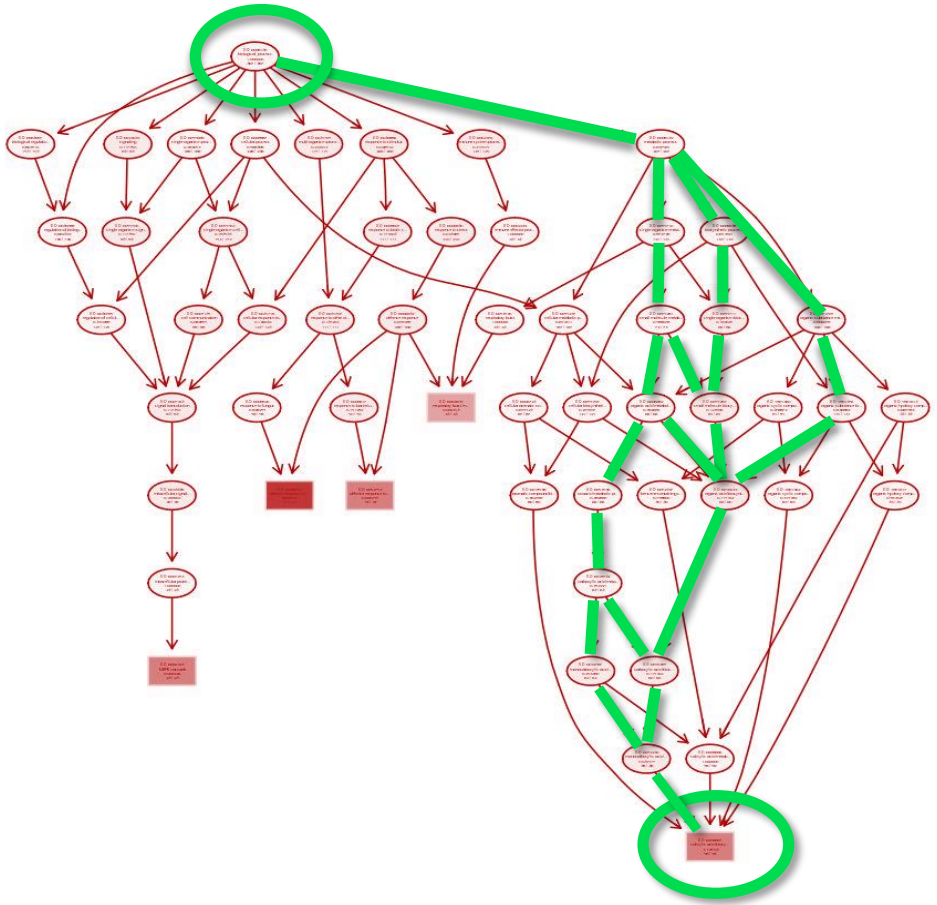
智能制造

仓储管理、零件生命周期监控

抽象模型：存证

多方共同鉴证：数据的产生时间，经手人，完整性，有效性，无篡改

抽象模型：追踪资产来龙去脉



- 区块链上保存了所有交易历史
- 每个交易都有参与者数字签名
- 交易的输入来自上一个有效的输出（UTXO）
- 交易一旦确认即被多方同步存储

✓ 数据完备，只增不减
✓ 来龙去脉，环环相扣，
✓ 多方鉴证，不可否认

可用于溯源追踪，反洗钱，版权保护等

抽象模型：公共账本

一致性账本

- 采用共识算法维护高度一致的账本，**无需额外对账**
- 一旦交易被确认，账本就被同步更新。

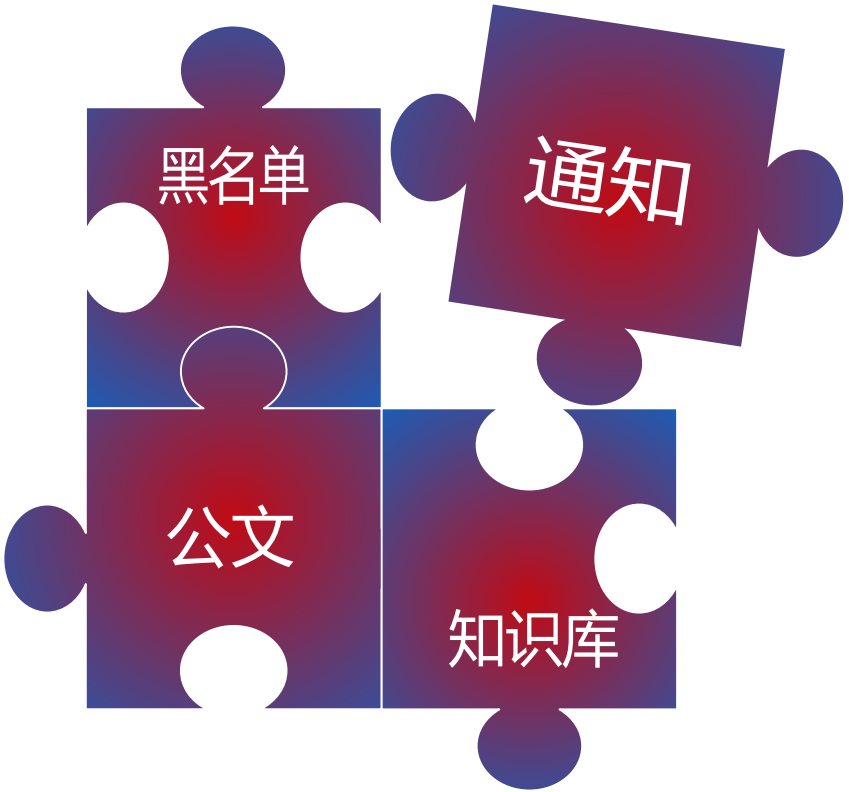
复式记账

- 有借必有贷，账目具有高一致性，头寸管理更加容易
- 只关注资金总账明细帐和流水，可不关注资产的唯一标识

通兑汇率

- 链上采用通用记账符号，降低流通复杂度
- 在多种资产交互时（如跨境或跨链交易），提供汇率支持

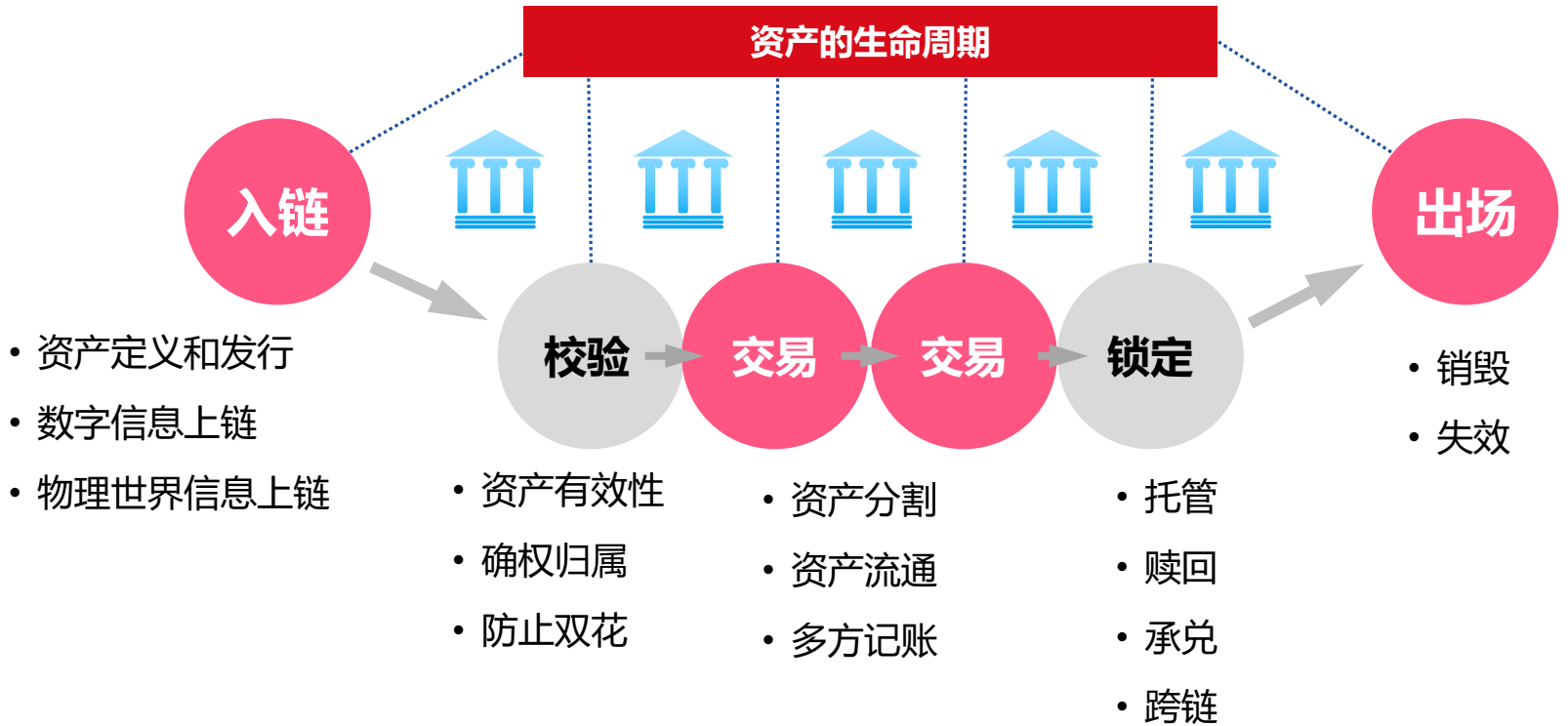
抽象模型：信息共享



- 数据可快速全网传播
- 传播路径可追溯
- 数据具有高度一致性
- 数据有分布式多备份
- 数据可确权

资产交易管理

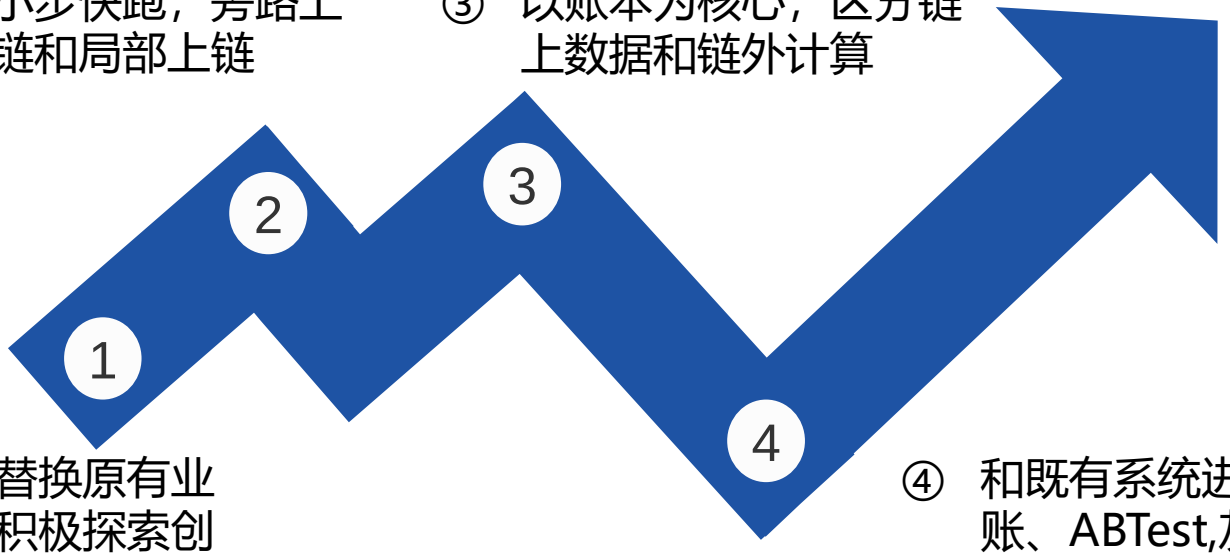
- 可用于票据，理财，信用证，债券，固定资产等交易管理



稳妥落地的业务实践路线

② 小步快跑，旁路上链和局部上链

③ 以账本为核心，区分链上数据和链外计算



① 不是简单替换原有业务，而是积极探索创新场景

④ 和既有系统进行整合、对账、ABTest,灰度发布

WeBank

谢谢！