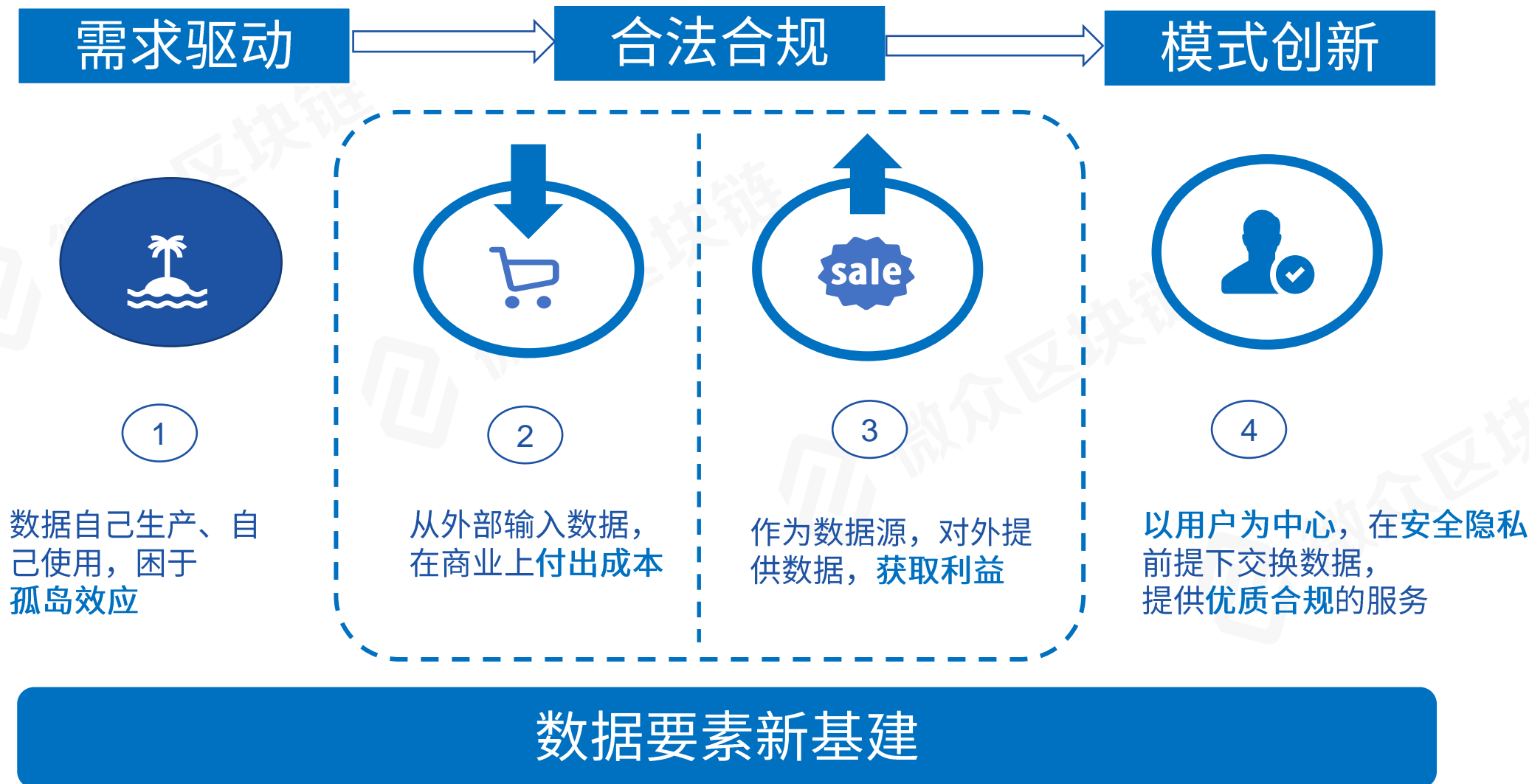




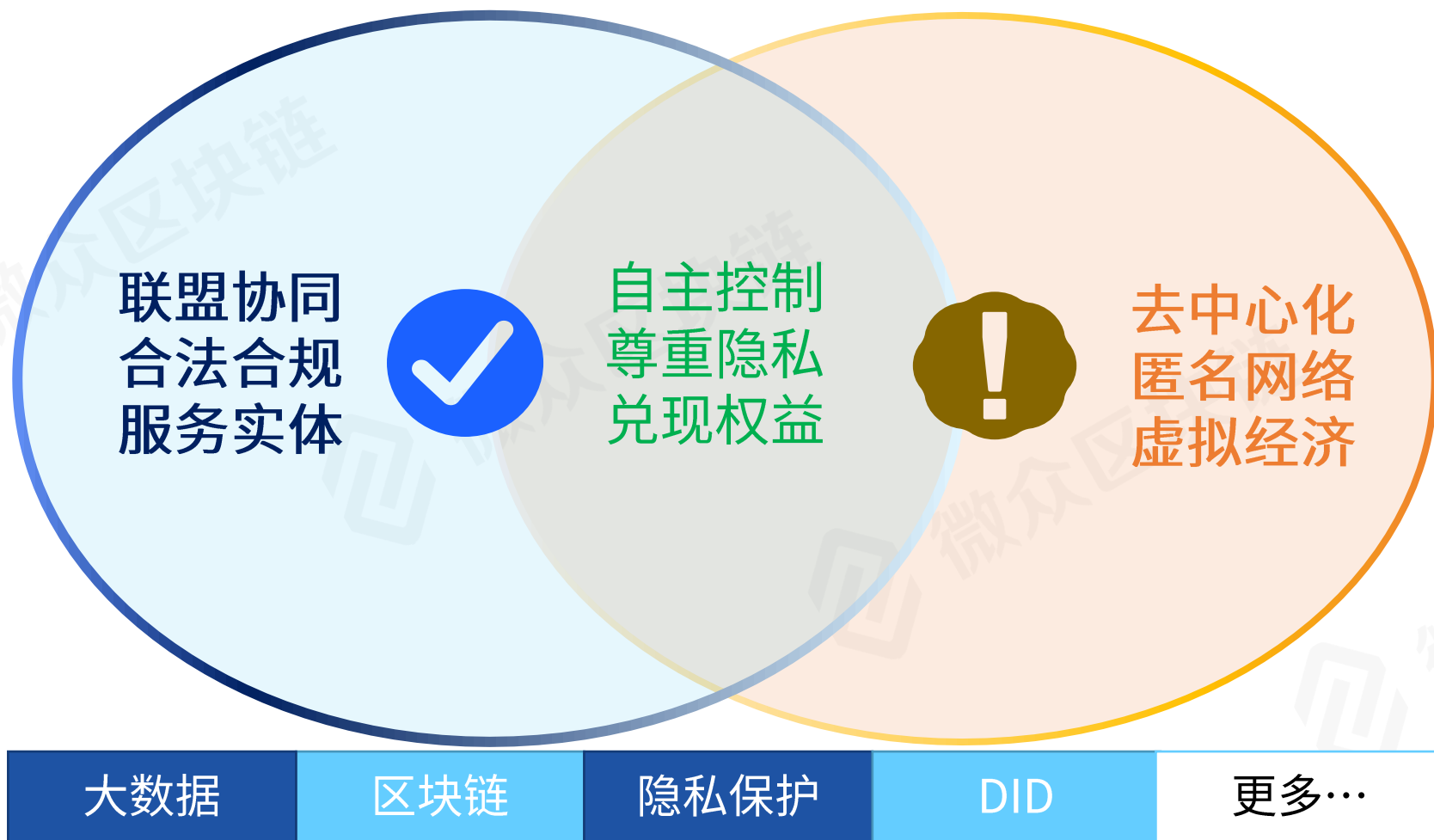
区块链融合隐私计算 迎接数据新基建

微众银行区块链首席架构师 张开翔

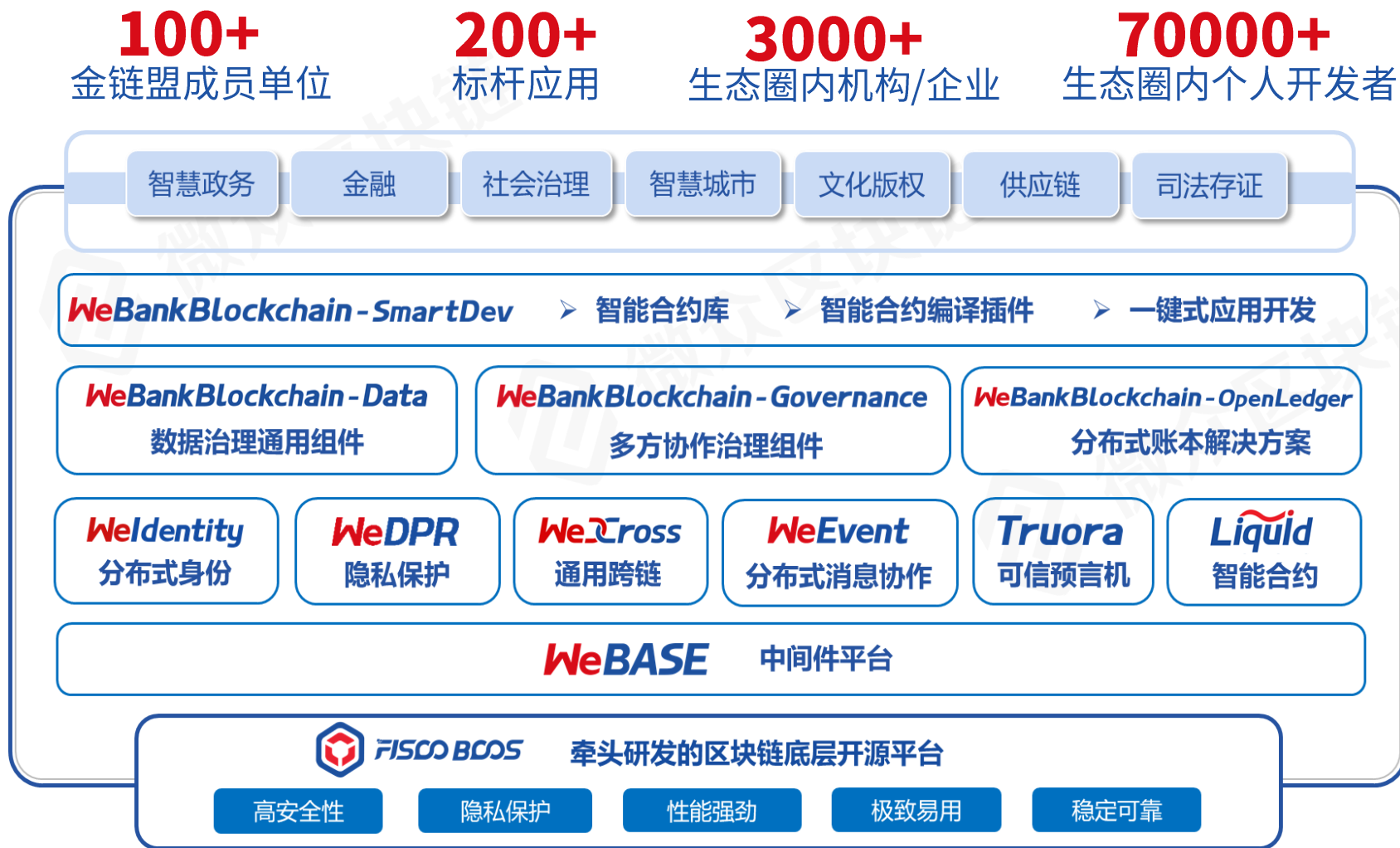
数据安全新规下的数据新基建



◆◆ 技术中立、风控优先的发展取向



构建面向数据新基建的全栈技术架构



7年研发历程

- 2015年投入研究
- 2017年全面开源



12个主项目

- 120+个开源仓库



领域全覆盖

- 联盟链底层平台
- 云原生中间件
- 核心解决方案
- 应用建设运营
- ...

安全可控的开源区块链生态加速产业落地



全面提速



标准化、易集成



上链更简单



可视化体验



链上数据智能化分析

效率提升

100%

用时节省

80%

流程便捷

5步

区块链应用 司法存证 供应链 溯源 文旅等

开发



合约IDE

应用构建

.....

运维



快速搭链

监控告警

.....

安全



账户私钥

权限控制

.....

数据



报表视图

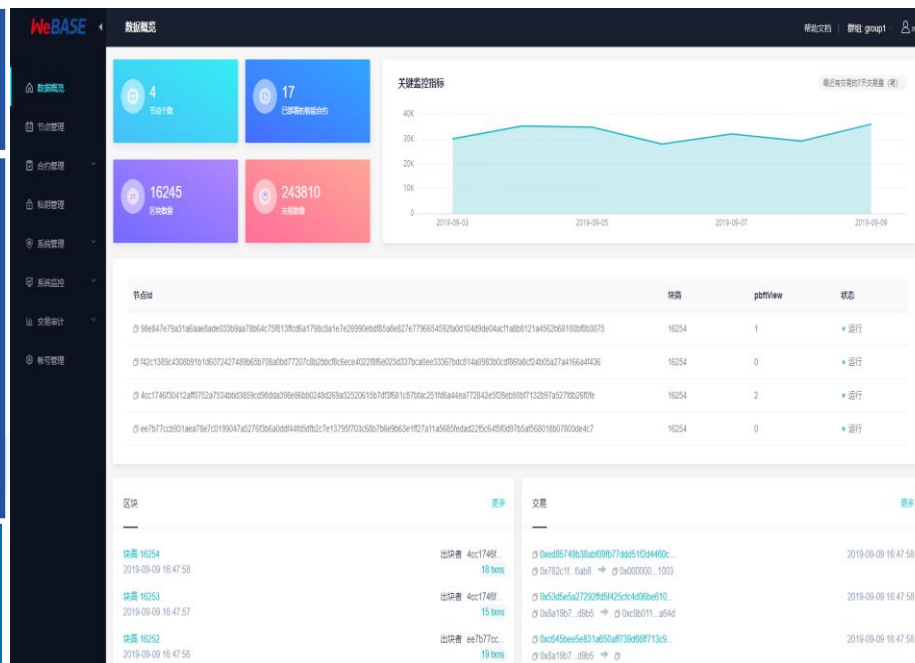
监管审计

.....

区块链底层平台



...



STEP 1
部署区块链节点

STEP 2
部署WeBASE

STEP 3
在线开发智能合约

STEP 4
调用API发送交易

STEP 5
使用管理平台运营

◆◆ 实现完整国产化支持，达成全方位安全可控

计算 > 网络 > 存储 全链路采用国密

智能合约

应用间通信

共识机制

节点间通信

存储加密

签名、验签

国密SSL通信协议

国密证书



采用国密算法和软硬件体系

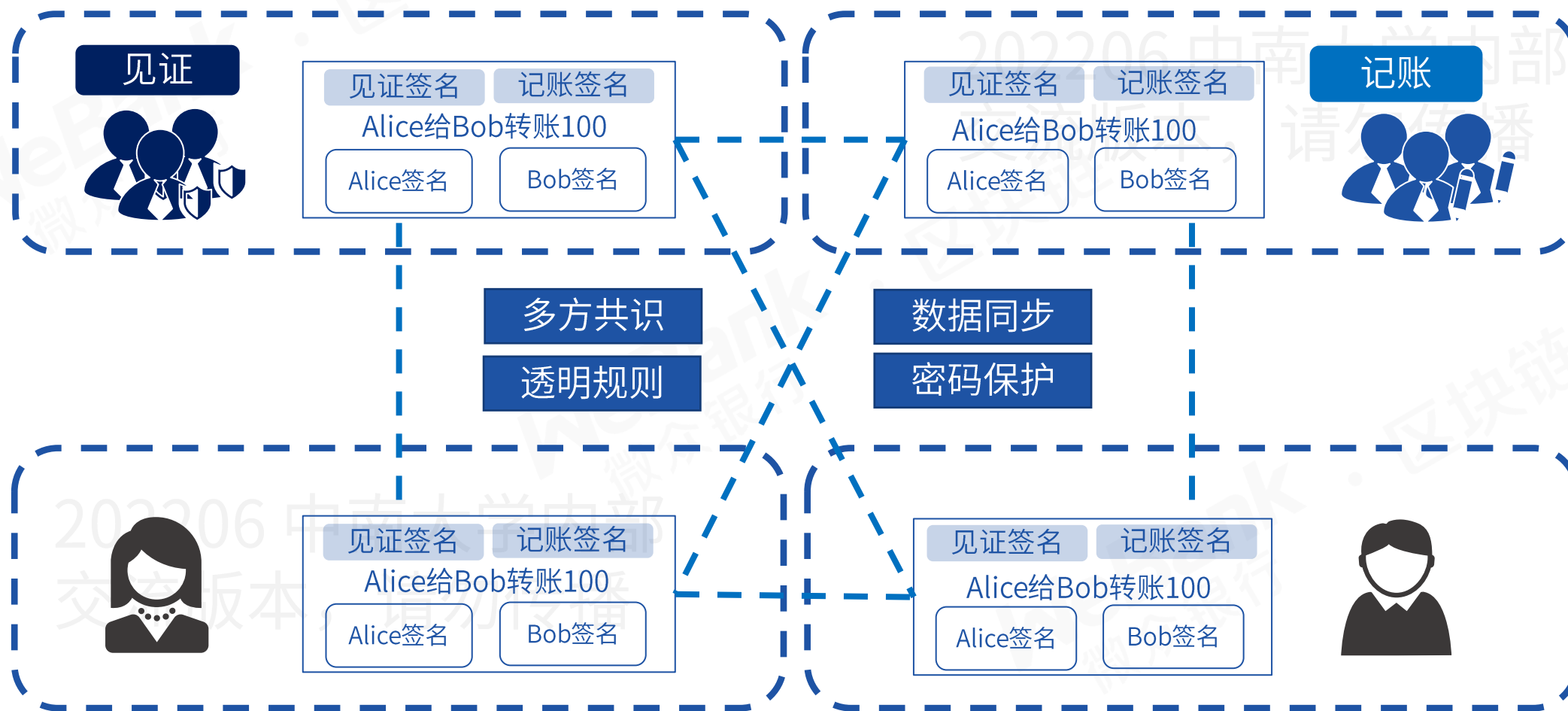


支持国产操作系统



适配国产芯片和服务器

◆◆ 分布式、多中心的协作模式



◆ 多方协作里的核心诉求



◆◆ 博大精深的密码学

Hash(哈希)算法	对称非对称加密	保护身份	隐私保护	前沿方向
<ul style="list-style-type: none">• SHA256• 大量数据的唯一摘要值• 作为数据的验证凭据	<ul style="list-style-type: none">• AES,RSA,ECC• 保护数据• 数字证书• 数字签名	<ul style="list-style-type: none">• 环签名• 群签名• 盲签名• 多方签名	<ul style="list-style-type: none">• 同态算法• 零知识证明• 安全多方计算	<ul style="list-style-type: none">• 属性加密• 格密码学• 量子密码学

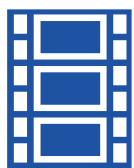
密码学是区块链和隐私计算的基础

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

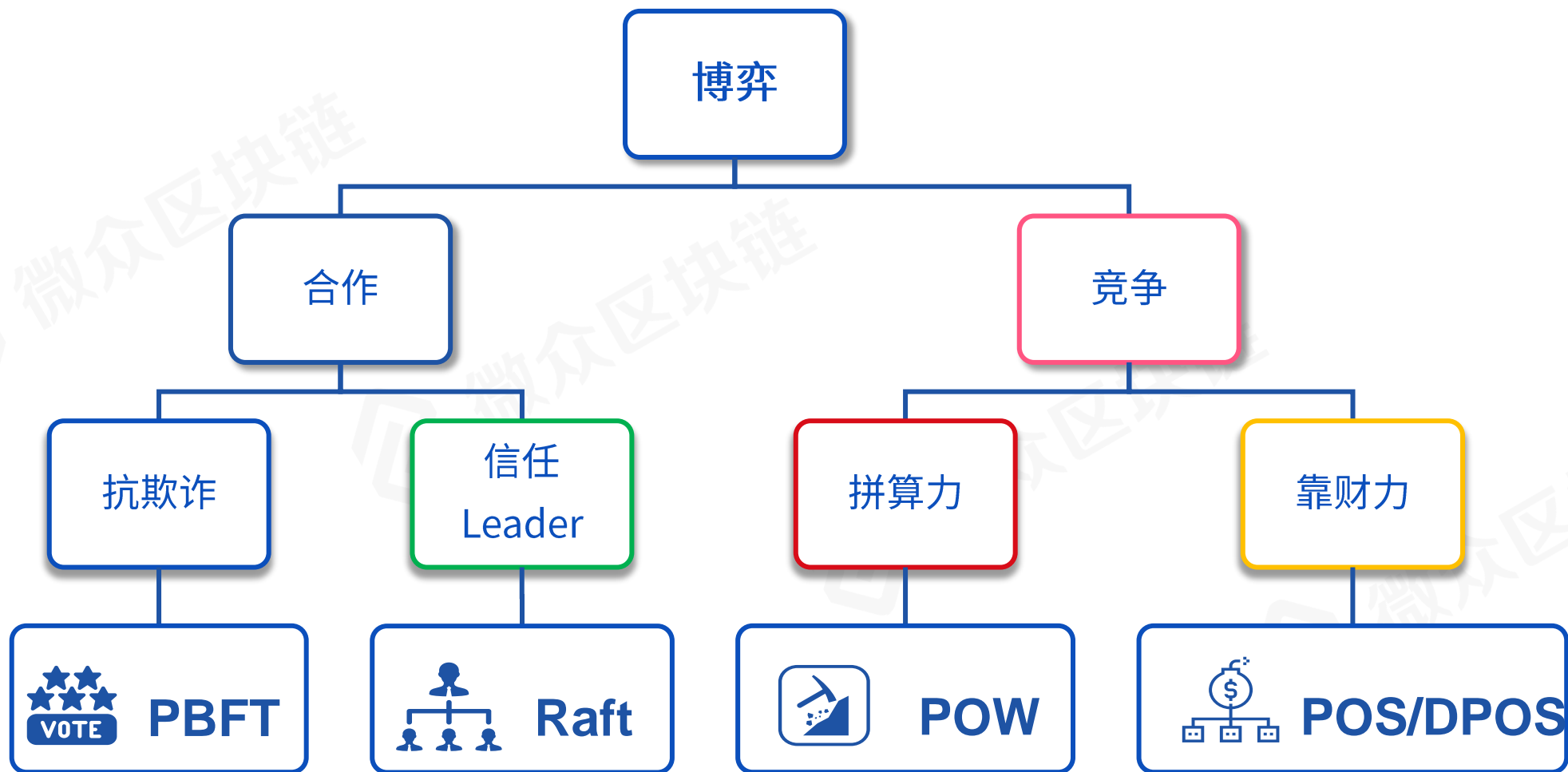
数字签名:
所有者确权

◆◆ 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

共识算法的选择



投票与协作

跟随Leader

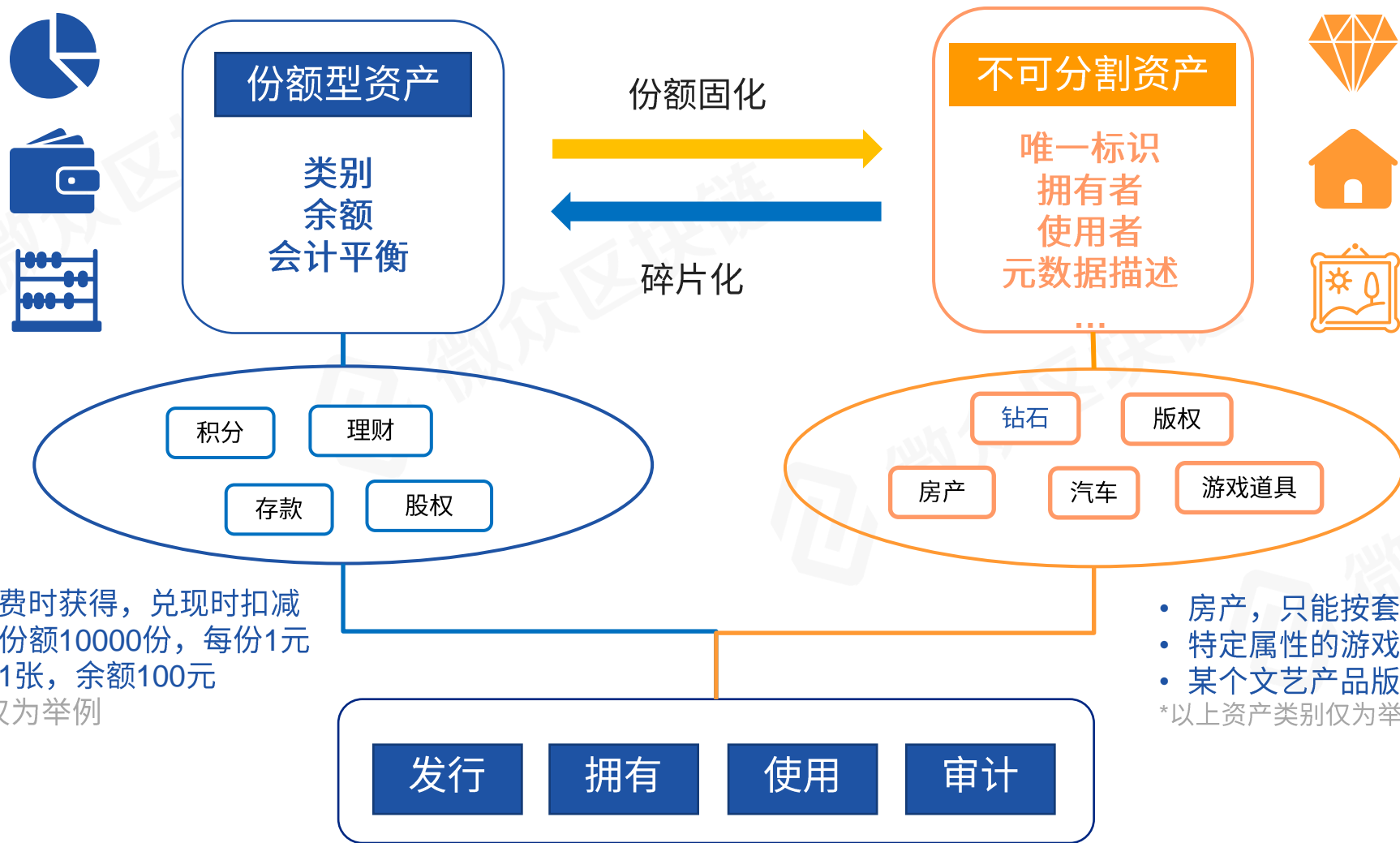
算力竞争

权益竞争

◆◆ 在分布式协作中智能合约的运用



采用智能合约实现不同的数字资产类型



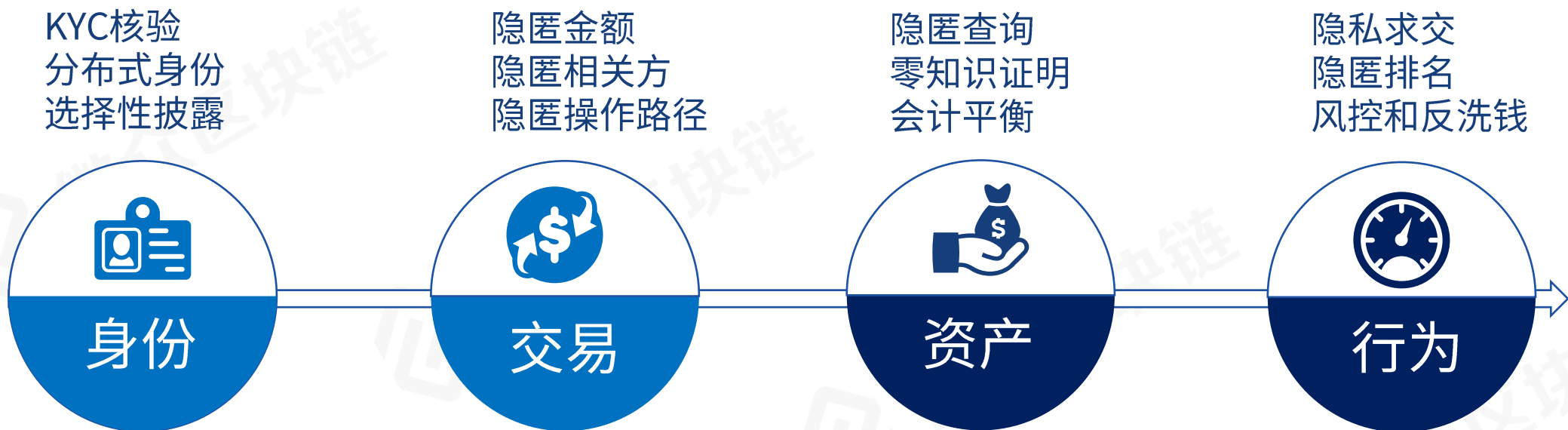
- 消费积分，消费时获得，兑现时扣减
- 某种理财产品份额10000份，每份1元
- 某商店充值卡1张，余额100元

*以上资产类别仅为举例

- 房产，只能按套为单位转让
- 特定属性的游戏道具
- 某个文艺产品版权

*以上资产类别仅为举例

分布式账本数据和隐私体系



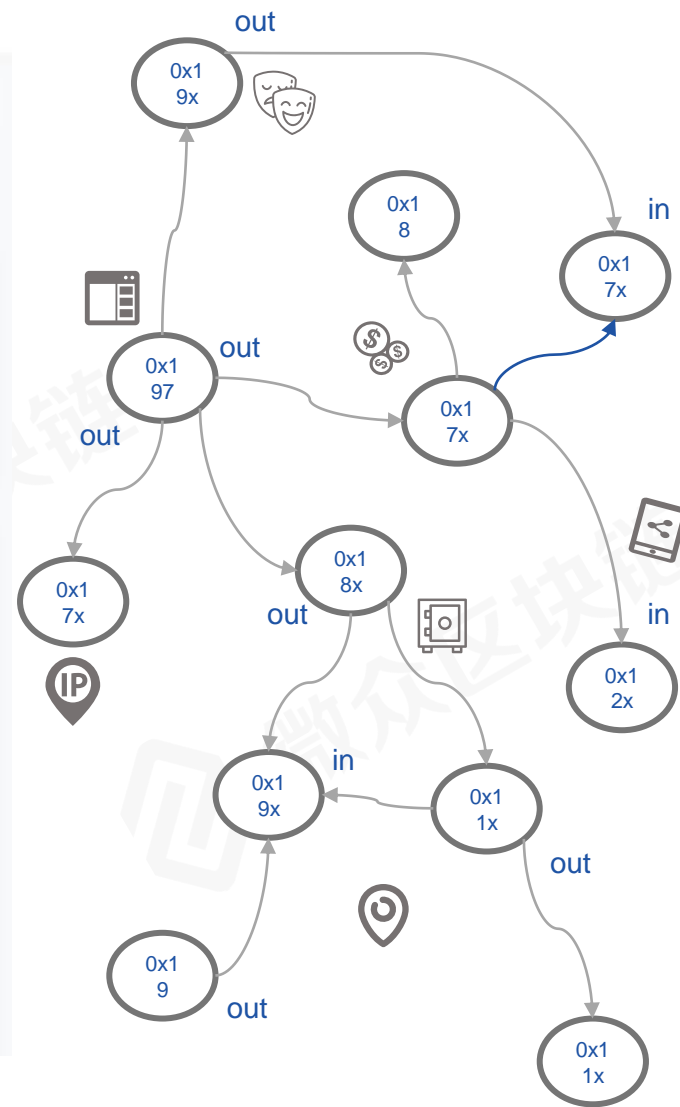
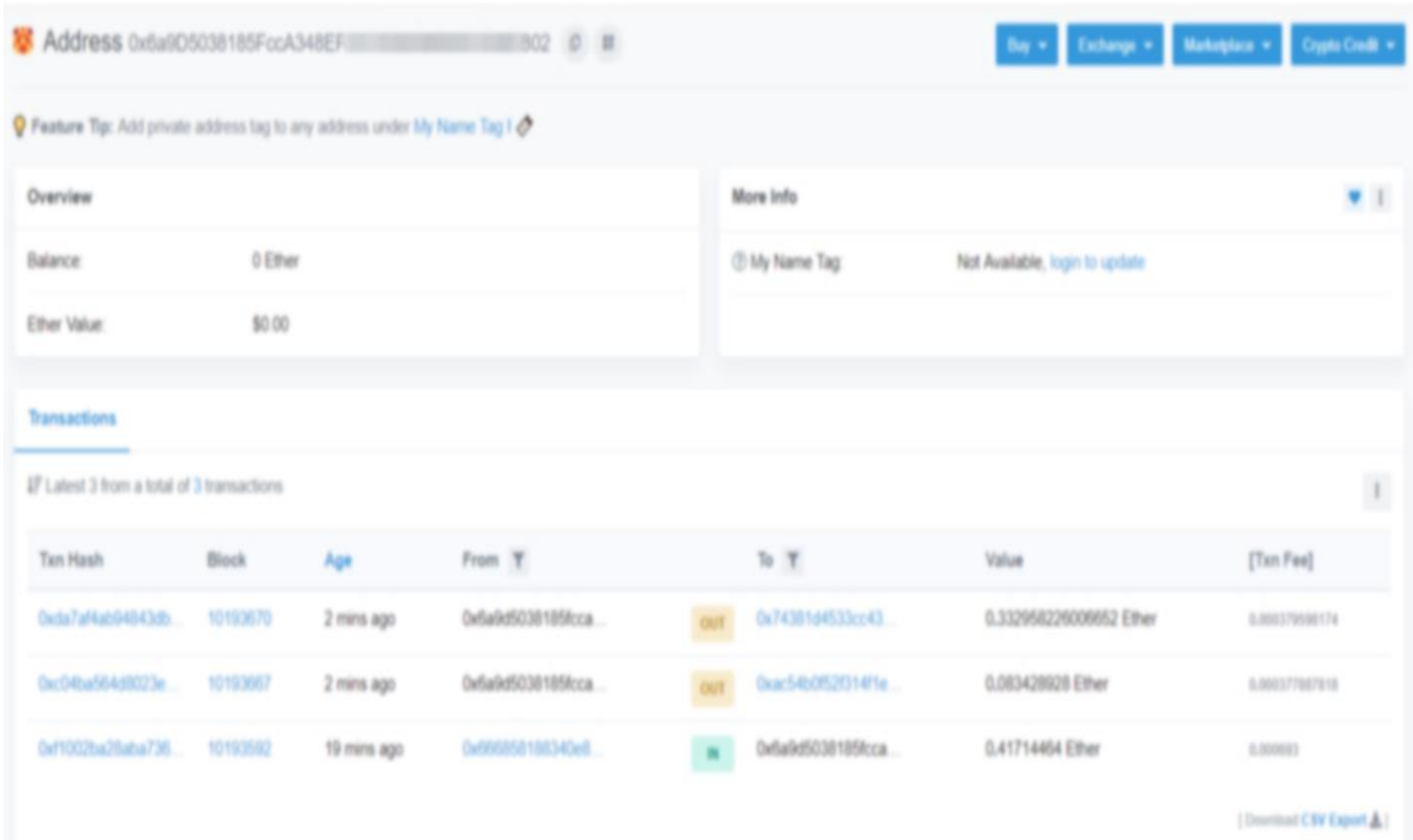
* 前台匿名，后台可控实名，联合隐私计算，支持监管审计



用户数据选择性披露
资产数据分级别保护



区块链的公开透明和隐私保护的权衡

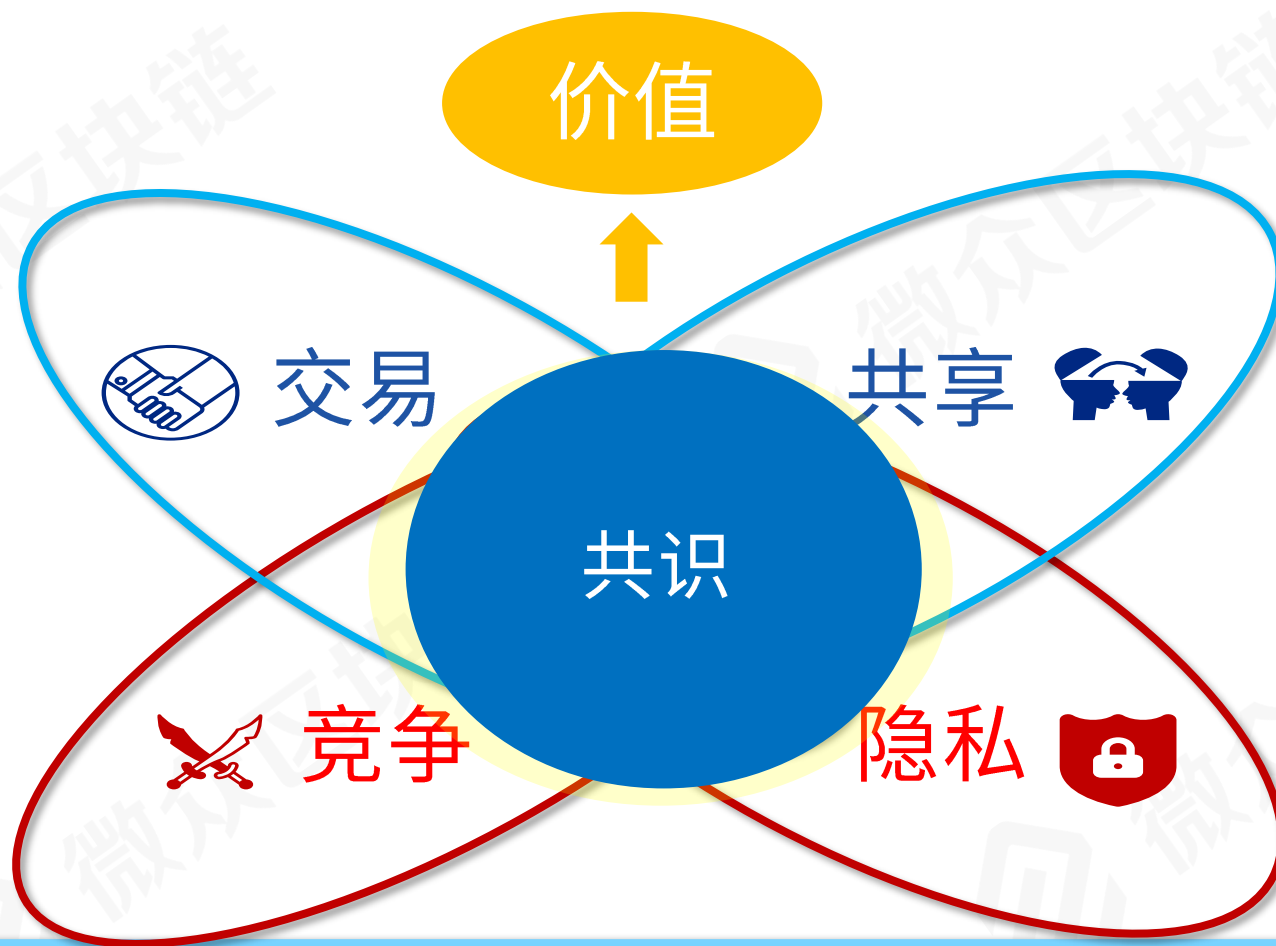




探寻博弈和价值体系的平衡

➤ 治理

- 建：谁来组建？
- 建：谁写合约？
- 建：谁做运维？
- 用：谁发交易？
- 用：谁记总账？
- 用：谁来验证？
- 管：谁做运营？
- 管：谁能加入？
- 管：谁来监管？



➤ 数据

- 链上有什么原生数据？
- 哪些实体数据会上链？
- 哪些数据泄露隐私？
- 用什么策略保护隐私？
- 成本和收益如何取舍分配？

什么是信任？求最大公约数？共享公共知识？Hash共识和联合计算？

个人场景的可控匿名和隐私保护



小明
18岁
男
计算机系

知道全部数据

证明小明是本校计算机系学生，本科学历，男，21岁，可以办证



小明
18岁
[Redacted]
计算机系

知道是谁，知道部分数据，且符合要求，


证明小明是本校学生且是21岁，所以可以办证



小明
≥18岁
[Redacted]
本校

知道是谁，知道范围数据，满足要求

证明小明是本校学生且已经年满18岁符合办理大学借书证的资格



DID
[Redacted]
CERTIFIED

只知道符合要求，不知道是谁(可控匿名)

证明某个人已经满足办理大学借书证的资格(零知识)

区块链+大湾区一体化：粤澳健康码跨境互认

后台服务不互联的前提下，如何完成跨境的信息验证？

- 2020年7月15日起，粤澳两地居民通关可免除14天医学观察期
- 目前已服务数以亿计人次通关
- 该跨境互通互认机制被写入2021年出版的重要读物《中国共产党简史》



粤澳恢复正常通关“健康码互认”保驾护航

2020-09-28 08:16

“粤康码”与“澳门健康码”互认系统于5月10日启用，目前已上线四个月有余。为加快恢复内地与澳门人员正常往来工作部署，自7月15日起，从粤澳口岸进入广东省人员免除14天医学观察，两地居民持粤康码通关凭证以及有效核酸检测阴性结果即可正常通关。

记者从广东省政务服务数据管理局了解到，“粤康码”通关凭证获取从最初的多屏填写、多次转码到现在自动填充，一扫扫码，全过程平均时长约1分40秒，再次通关时获取通关凭证不超过3秒即可完成，实现“快速转码、亮码通关”。截至目前，持粤康码通关凭证通关累计超900万人次。

■ 深圳特区报记者 邹媛

● 区块链技术构建可信通道

高效率通关的背后是科技的支持。两地健康码的跨境互认通过运用区块链等技术，让“数据不出境、健康码互认”成为可能。应用满足验证健康信息真实有效等需求的同时，保护个人信息隐私安全，不仅提升了通关旅客体验感、缓解了通关现场管理压力，也为入境人员后续健康服务管理提供了有力抓手，对支持两地人员正常往来和经济社会交流恢复发挥了关键作用。

后台服务不作互联

个人自愿提出转码

转码数据全程加密

链上验证信息可信

◆◆ 分布式数字身份 :多种技术的组合

场景:



分布式商业



社会治理



教育、医疗...

目的:



自主控制



分布式验证



隐私保护

角色:



认证者



用户



验证方

数据:



身份凭据



资质和信用



文本、图片、音视频

业务
表现



did:weid:101:0xae0b295667a9fd93d5f28d9ec85e40f4cb697bae



技术
支撑

协议:

DID Document

Credentials

Claim

Presentation

Policy

...

功能:



终端工具



数据可信管理



安全交换机制

平台:



中间件



区块链



分布式存储

算法:

分布式一致性算法

多态签名

MPC

零知识证明

同态加密

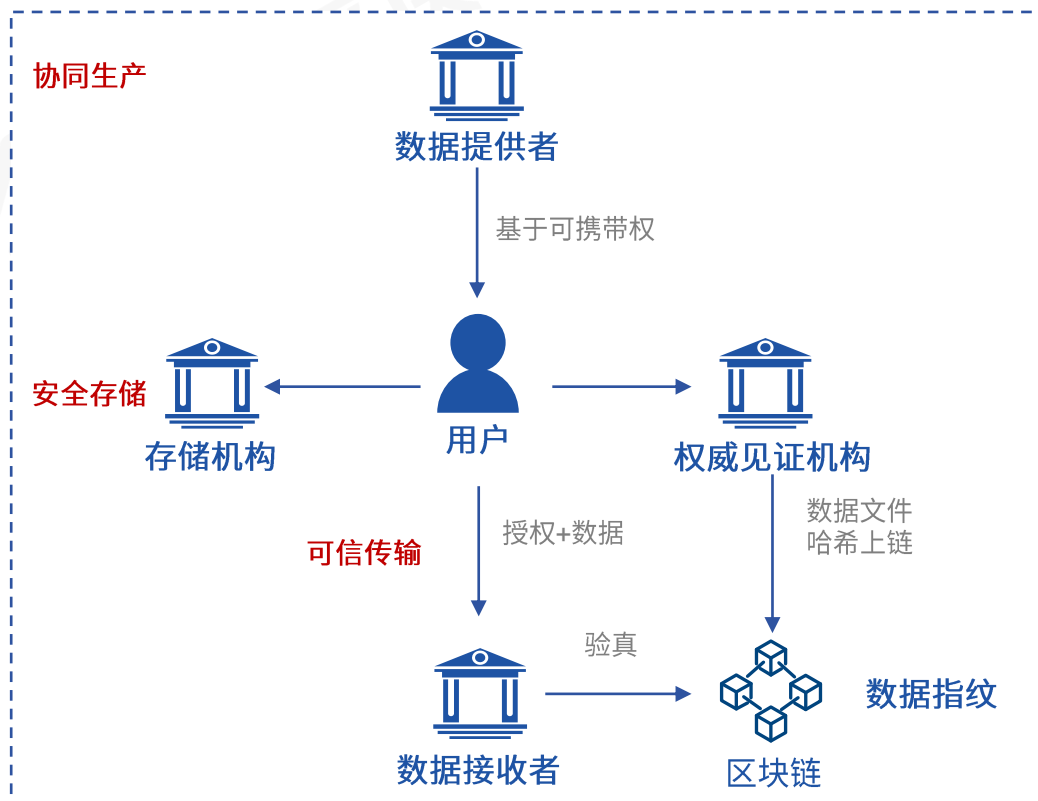
...

分布式数据传输协议DDTP

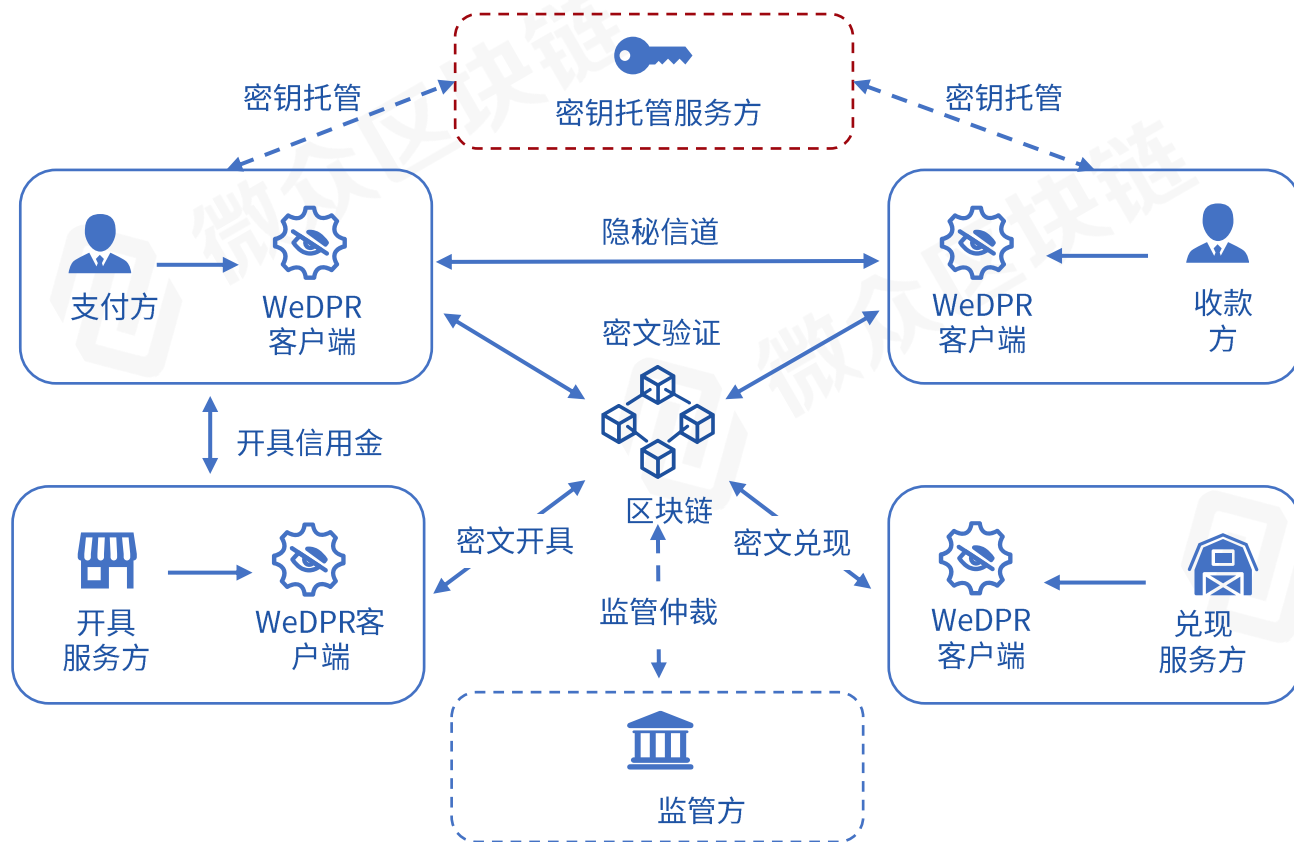
Distributed Data Transfer Protocol

让用户成为关键参与者

基于个人数据可携带权，**用户主动发起**个人信息数据传输并**自行上传**，基于**区块链**实现数据可信验真，传、验分离



匿名账本方案



• 身份隐匿:

用户资产或权益是流转的载体。权益拥有者在进行转账时可以不披露自己的身份，但是可以证实自己针对权益的所有权，并且可以给出权益与自己身份关联的证明。

• 权益隐匿:

除了交易双方，第三方不能知道权益凭证的内容，如交易金额。

• 交易隐匿:

除了交易参与者，第三方无法获知交易的具体细节，如交易参与方的信息，交易发起时间，签名等。

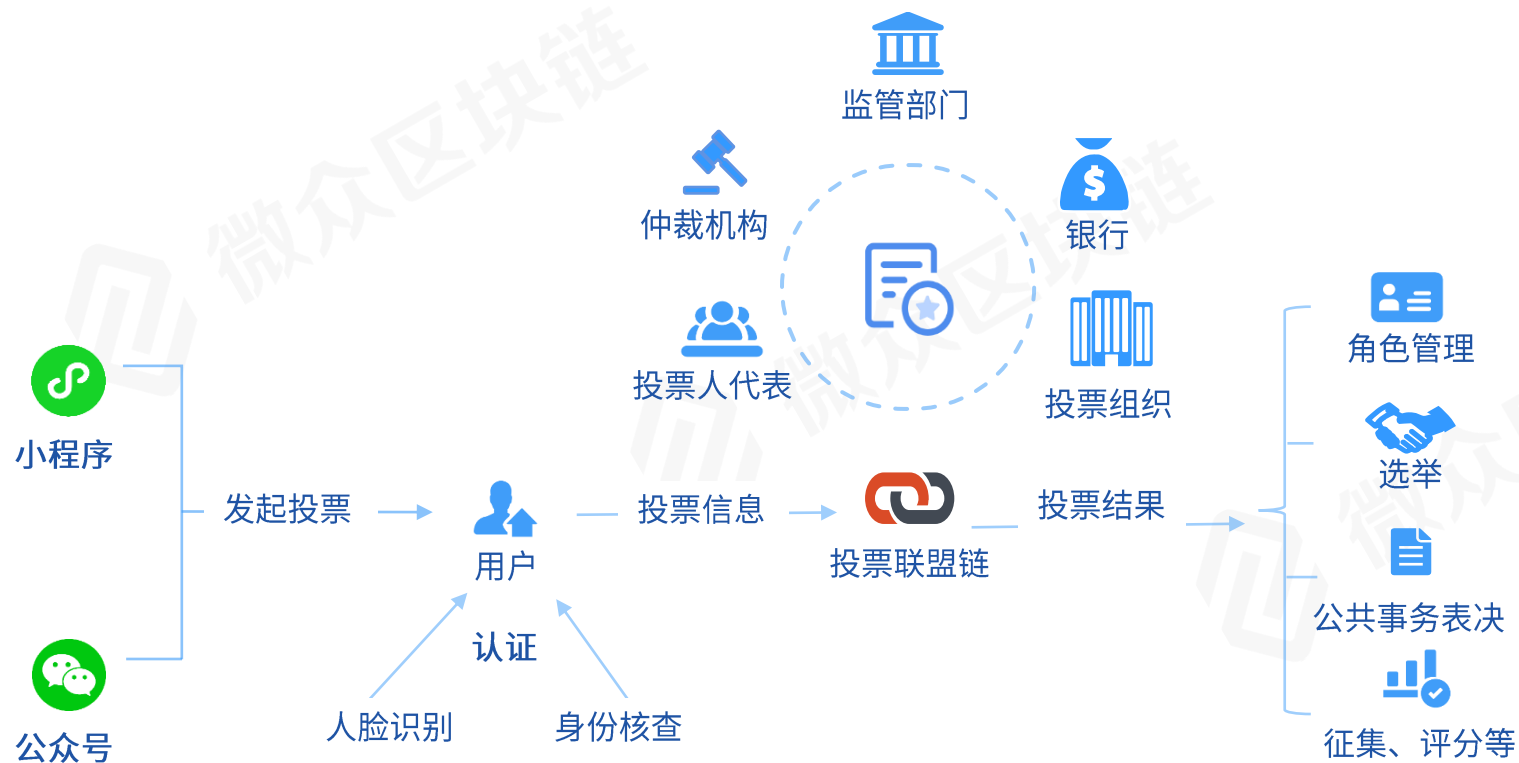
• 抗双花:

利用区块链的全局账本，同一份权益凭证不能被花费两次。

• 监管友好:

监管方可以在交易发生后的时刻获取必要的仲裁信息。

区块链+投票场景：隐私投票平台

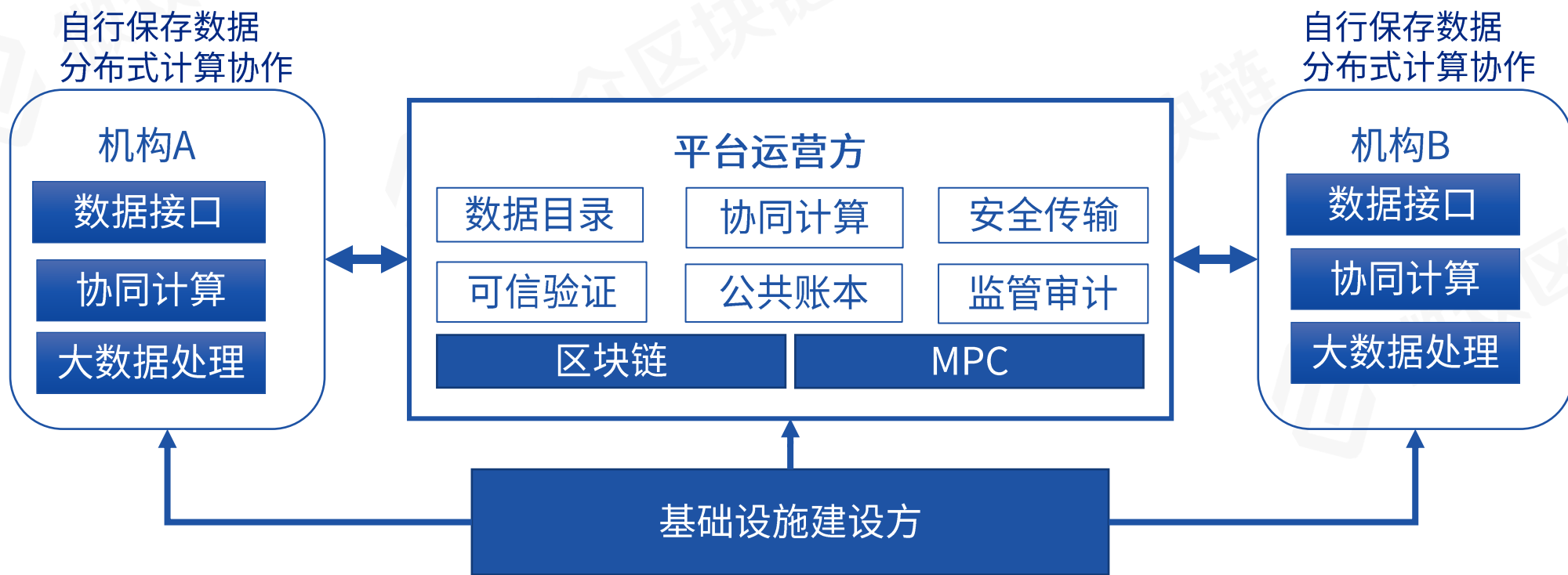


解决多方治理中涉众决策难问题

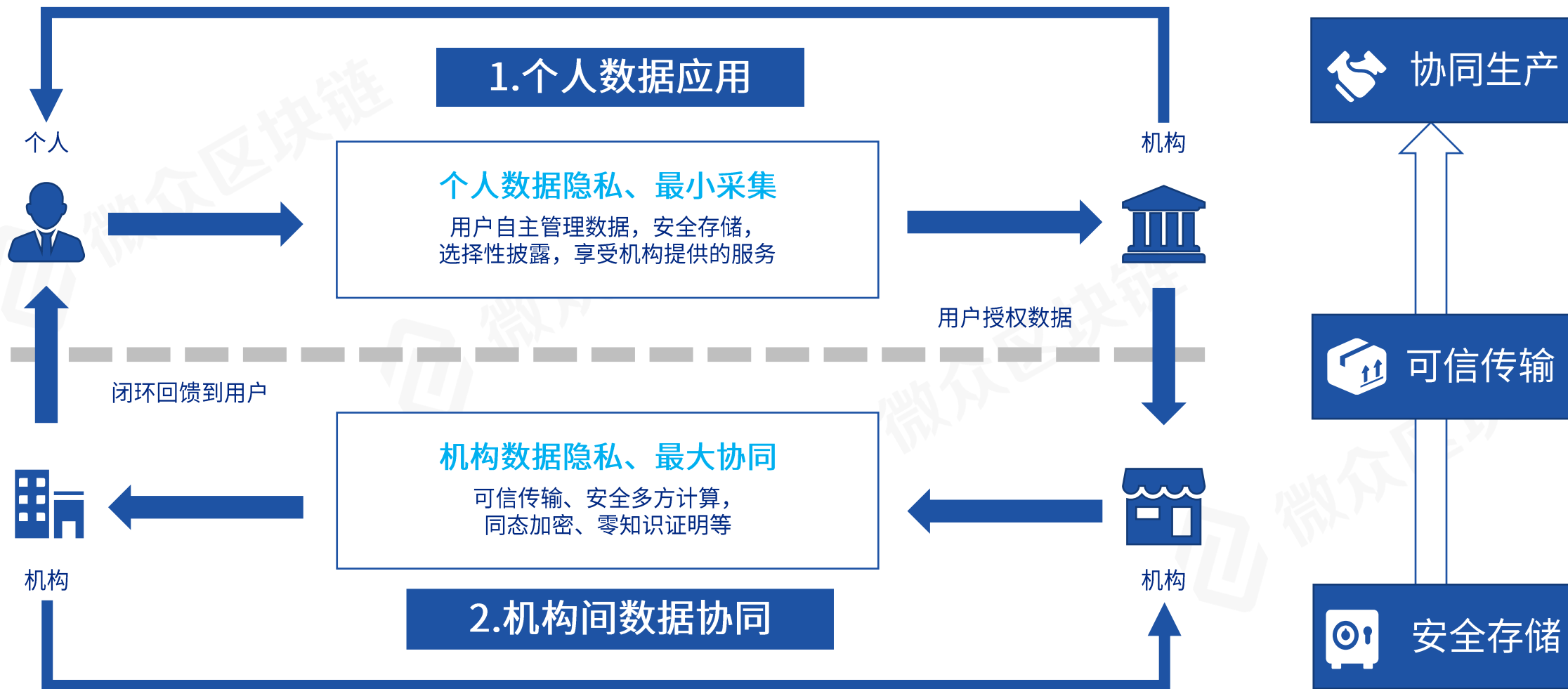
- 搭建投票人身份标识链，杜绝伪冒现象
- 隐匿投票人投票的具体数量和结果
- 可验证投票人投票有效且正确计票
- 监管、仲裁机构链上协作，具备公信力

◆ 机构之间的数据协作

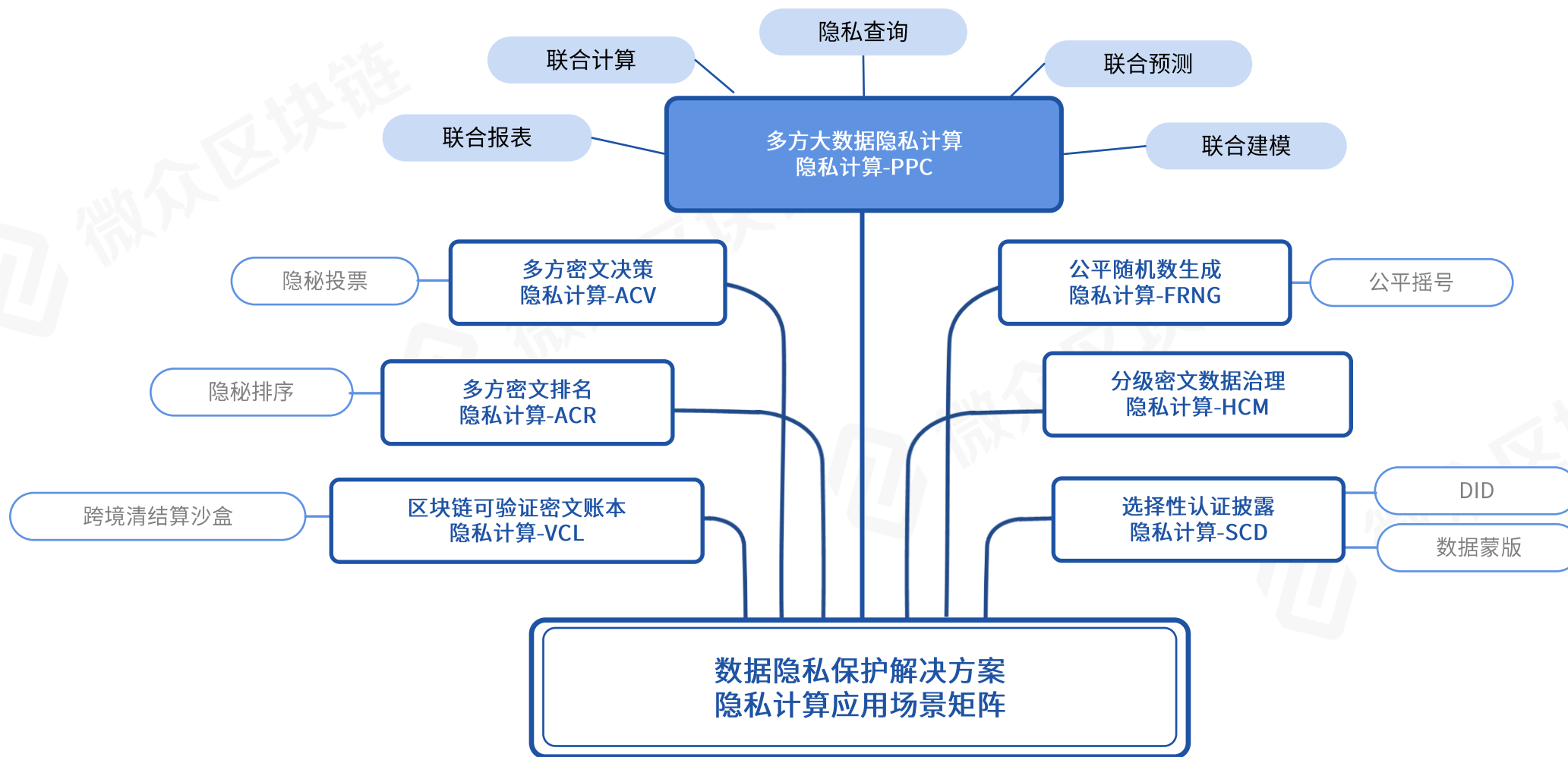
- 平台运营方是专业的机构或行业联盟，监管机构可接入到平台中
- 机构可以将数据索引和目录上报到平台方，或可选的在链外保存
- 机构间基于平台能力，实现受控的数据接口服务，通过多方安全计算协同，
- 最终，达成“可用不可见”的效果



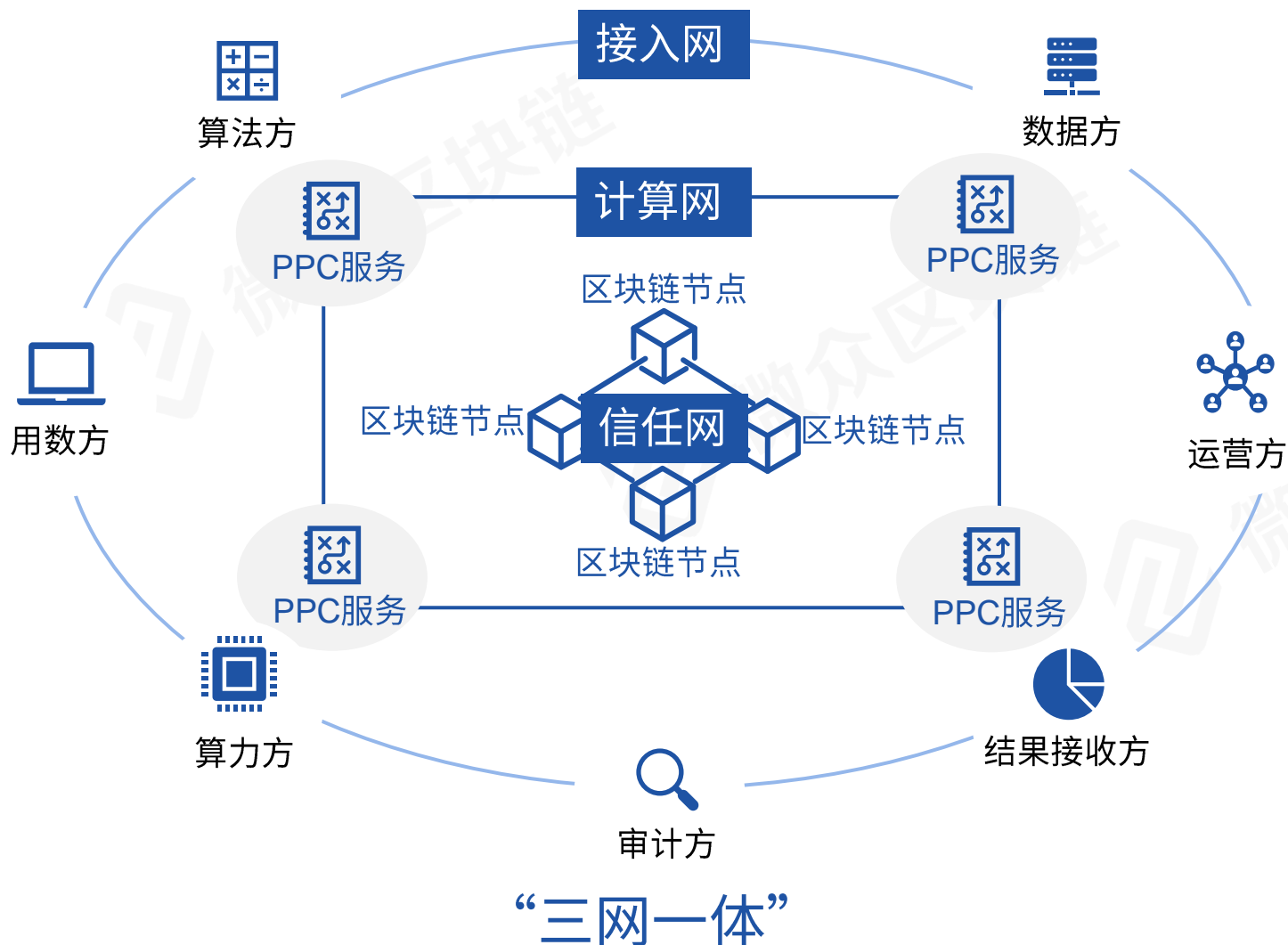
“双循环”实现隐私保护和数据流转



隐私计算体系：场景化的隐私保护能力



◆ WeDPR-PPC灵活支持双架构实现



数据方是否为计算方？

直连计算架构

适用场景：

- 参与方少
- 参与方完全对等
- 合作关系相对固定

优势：

- 私有化快速部署
- 易推广应用
- 监管友好

代理计算架构

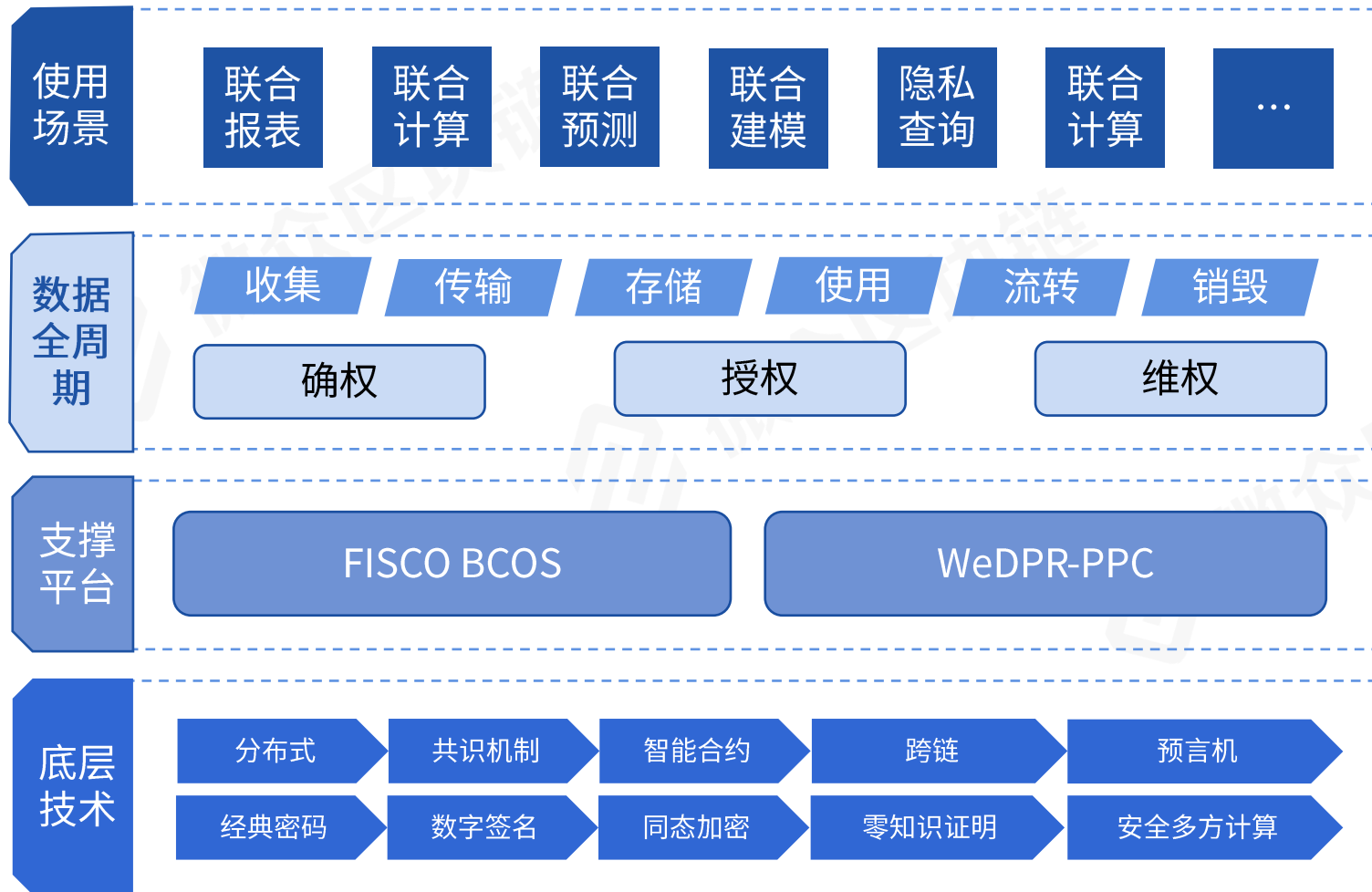
适用场景：

- 动态参与方
- 参与方资源不对等
- 业务协作动态变化

优势：

- 轻量部署
- 兼容直连计算
- 参与方扩展性强
- 规模经济效益
- 监管友好

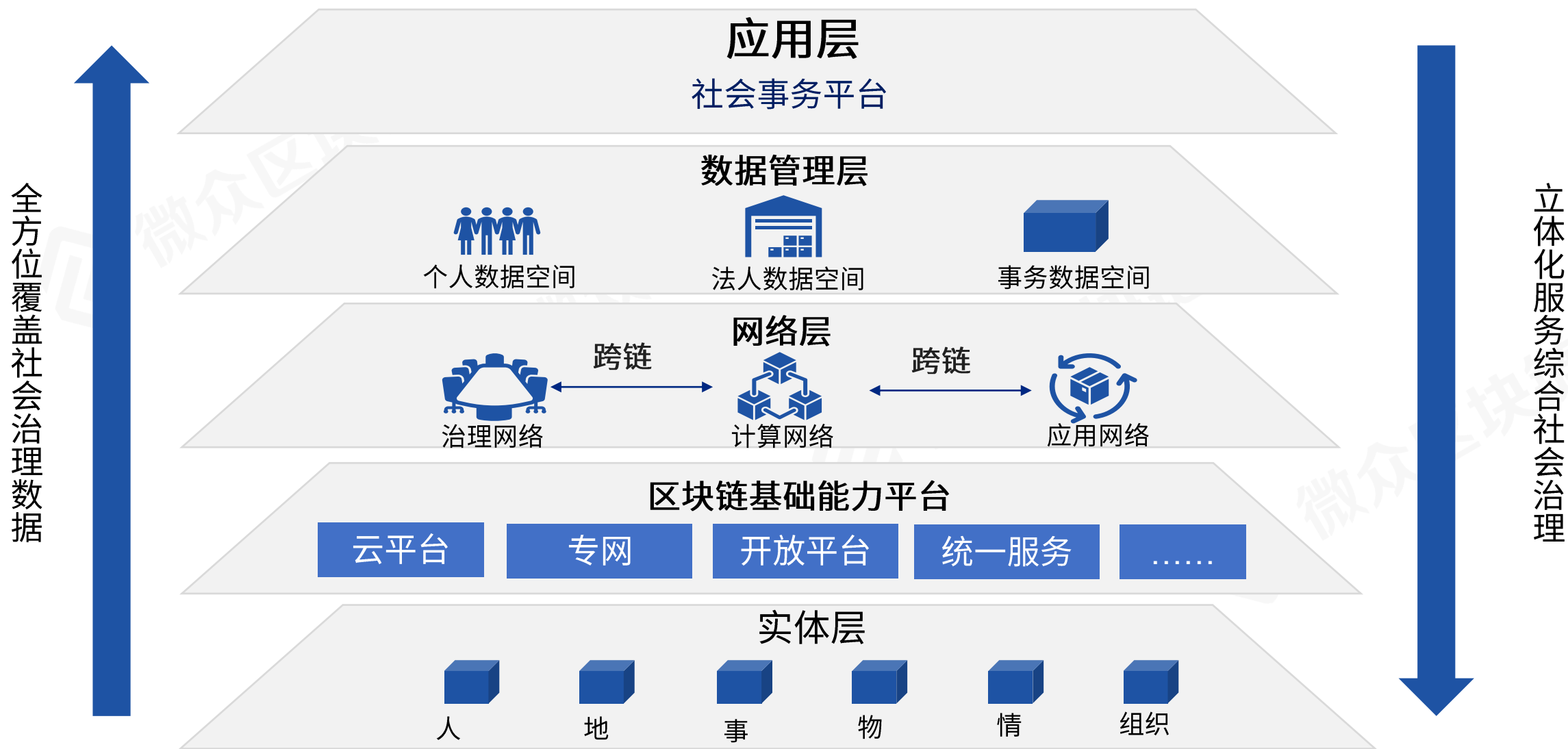
◆ WeDPR-PPC: 隐私计算平台



权威测评认证



数据新基建：融合多种技术和多层体系





微众区块链



应用案例

开发教程

进群交流

活动报名

合作联系