



公有区块链与区块链即服务

演讲人：维优CTO 陈浩

北京

伦敦

纽约

旧金山

圣保罗

上海

东京

QCon

全球软件开发大会

[上海站]

主办方 **Geekbang** 极客邦科技 **InfoQ**

信息安全

机器学习

人工智能

黑产

互联网金融 (FinTech)

团队管理

云计算

基础设施

软件性能

硅谷

微服务

互联网架构

2017年10月17-19日
上海·宝华万豪酒店

——> 扫描二维码
开启软件开发新思路





Geekbang> | EGO EXTRA GEEKS' ORGANIZATION NETWORKS
极客邦科技

EGO会员招募季

EGO旨在组建全球最具影响力的技术领导者社交网络，联结杰出的技术领导者学习和成长。

2017年6月30-7月10



扫码报名

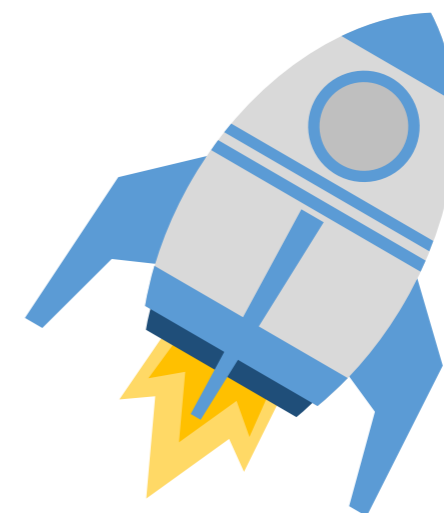
SPEAKER INTRODUCE

陈浩 维优CTO

- 拥有传统网络服务高并发架构经验和公有区块链架构双重经验。2016年初通过区块链医疗存证项目获得区块链黑客马拉松上海站第三名。
- 2016年主导并与团队设计实现了中国第一条公有链——Metaverse(元界)。2017年2月主网上线后，作为区块链底层支持黄金现货交易、艺术品传承、医疗等数个商业应用项目，4个月内市值迅速增长到5.5亿美元，全网算力达到400GH。
- 2016年主导并与团队设计实现了自己的数字资产交易系统——海枫藤(szzc.com)。2017年初上线后4个月内单日交易量突破千万，月交易量过亿，并且持续快速增长中。



目录



区块链技术简要



区块链的核心要素和发展趋势



公有区块链技术实践——Metaverse元界



区块链即服务——未来新架构模式

Part 1 区块链技术简要



区块链分类



区块链核心要素



区块链四个常见的技术栈



按许可性质分类



私有账本

- ✓ 传统数据库
- ✓ 私有区块链



联盟链

- ✓ HyperLedger
- ✓ R3 Corda
- ✓ EEA



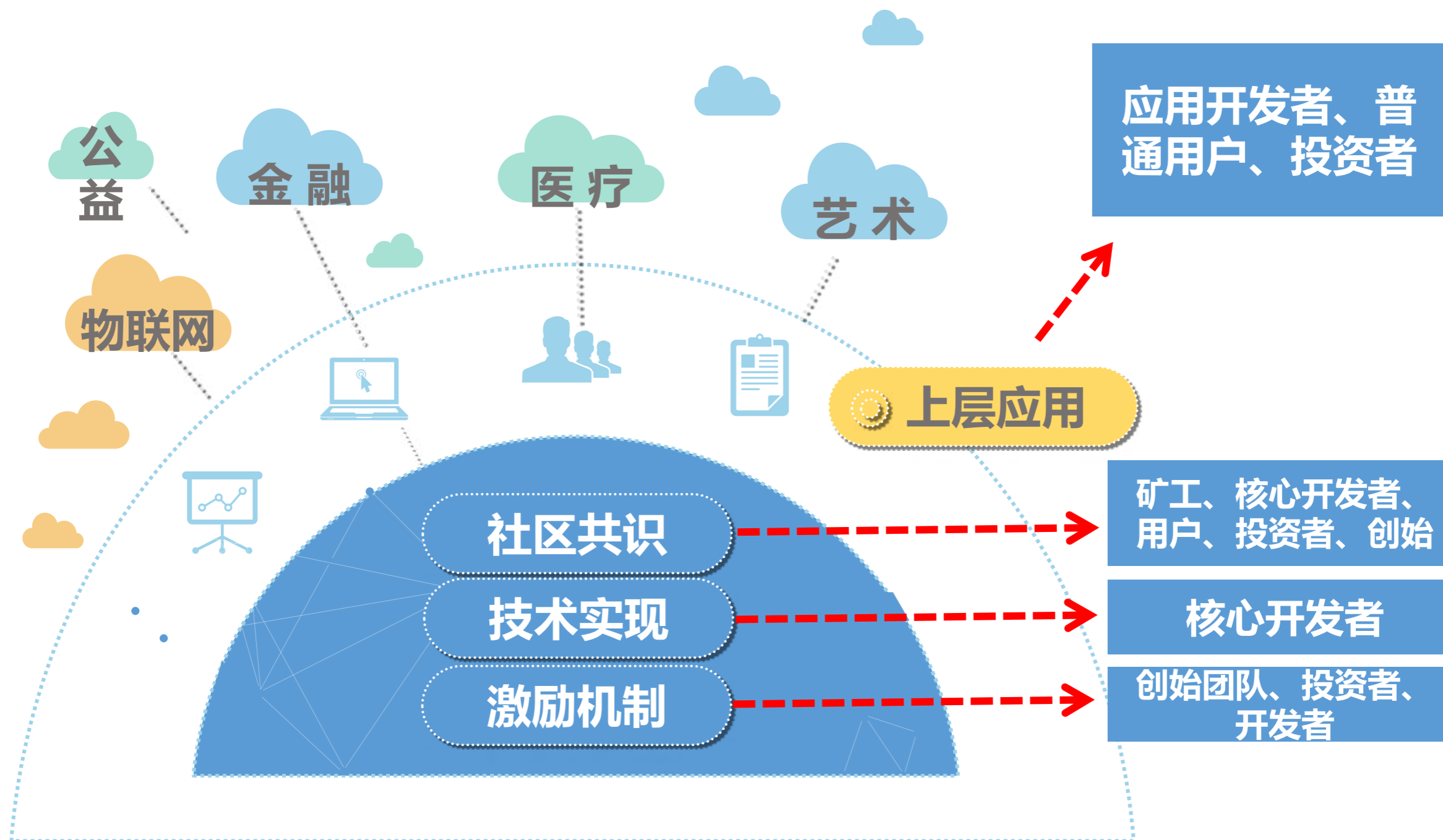
公链

- ✓ 比特币
- ✓ 以太坊
- ✓ 比特股
- ✓ 未来币

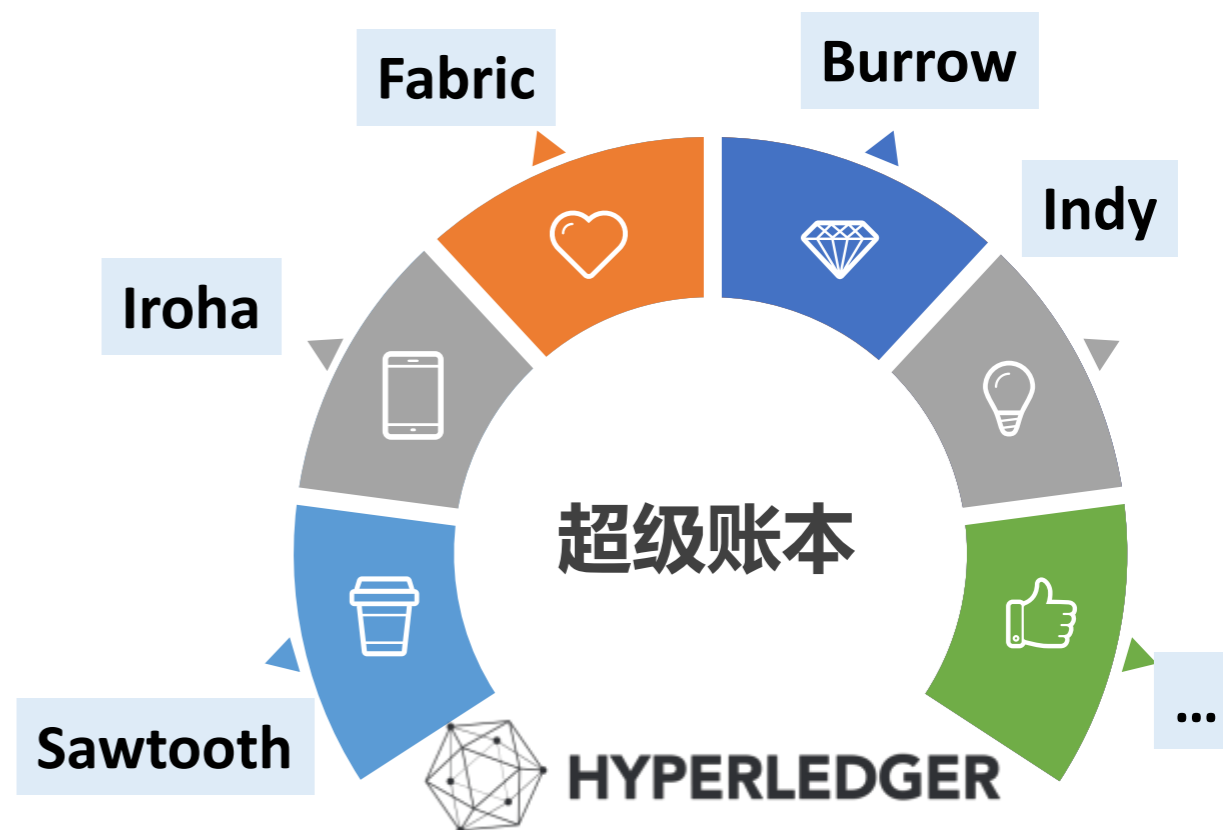
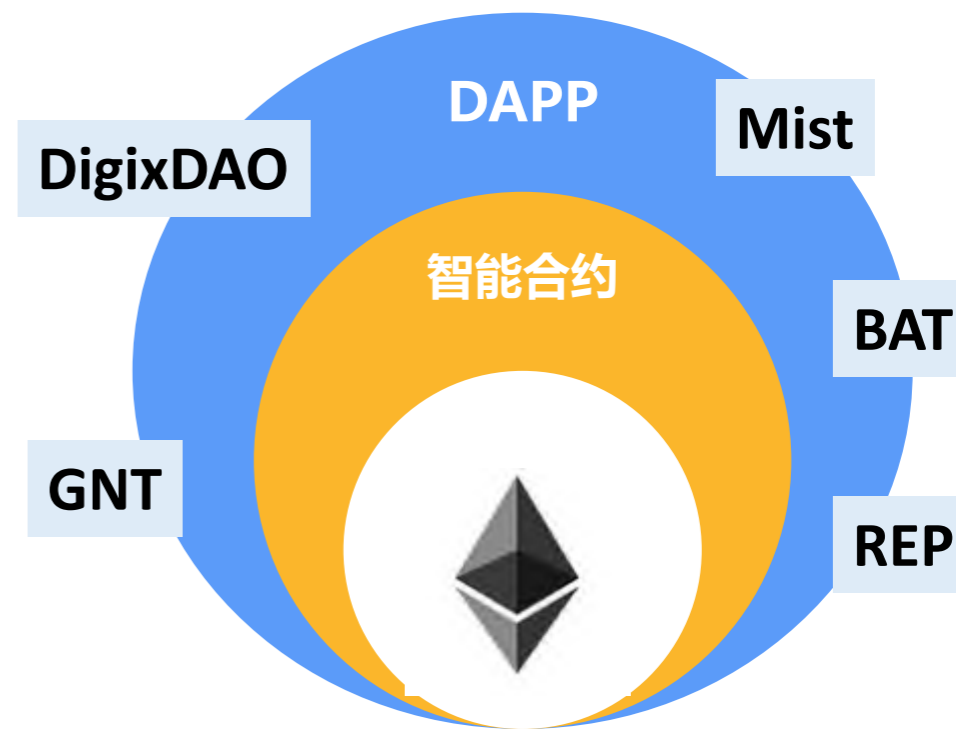
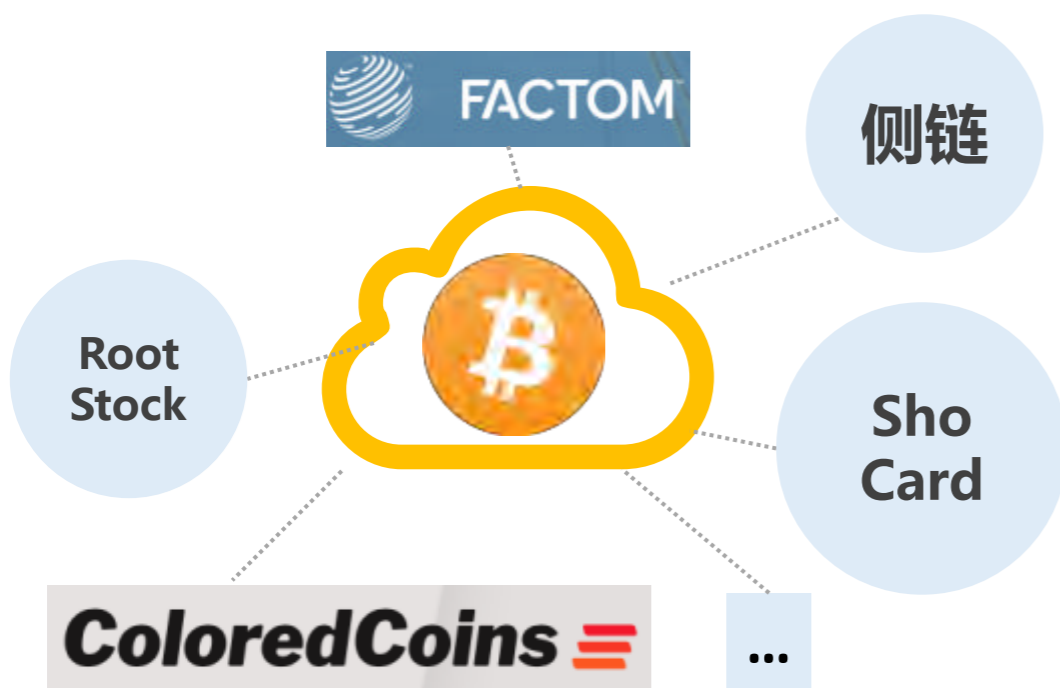
封闭

开放

公链核心要素



四个常见技术栈



Part 2 区块链的核心要素和发展趋势



核心技术要素



产品要素——

数字资产、数字身份和价值中介



区块链即服务



技术核心要素

1 P2P网络协议

- 动态演化稳定性
- 全网广播交易实时性
- 网络传输吞吐量



2 分布式共识算法

- 资产交割速度（初开时间和大小）
- 拜占庭容错阈值（51%攻击）
- 分叉频率



3 加密签名算法

- 加密强度
- 加解密性能
- 密码学标准



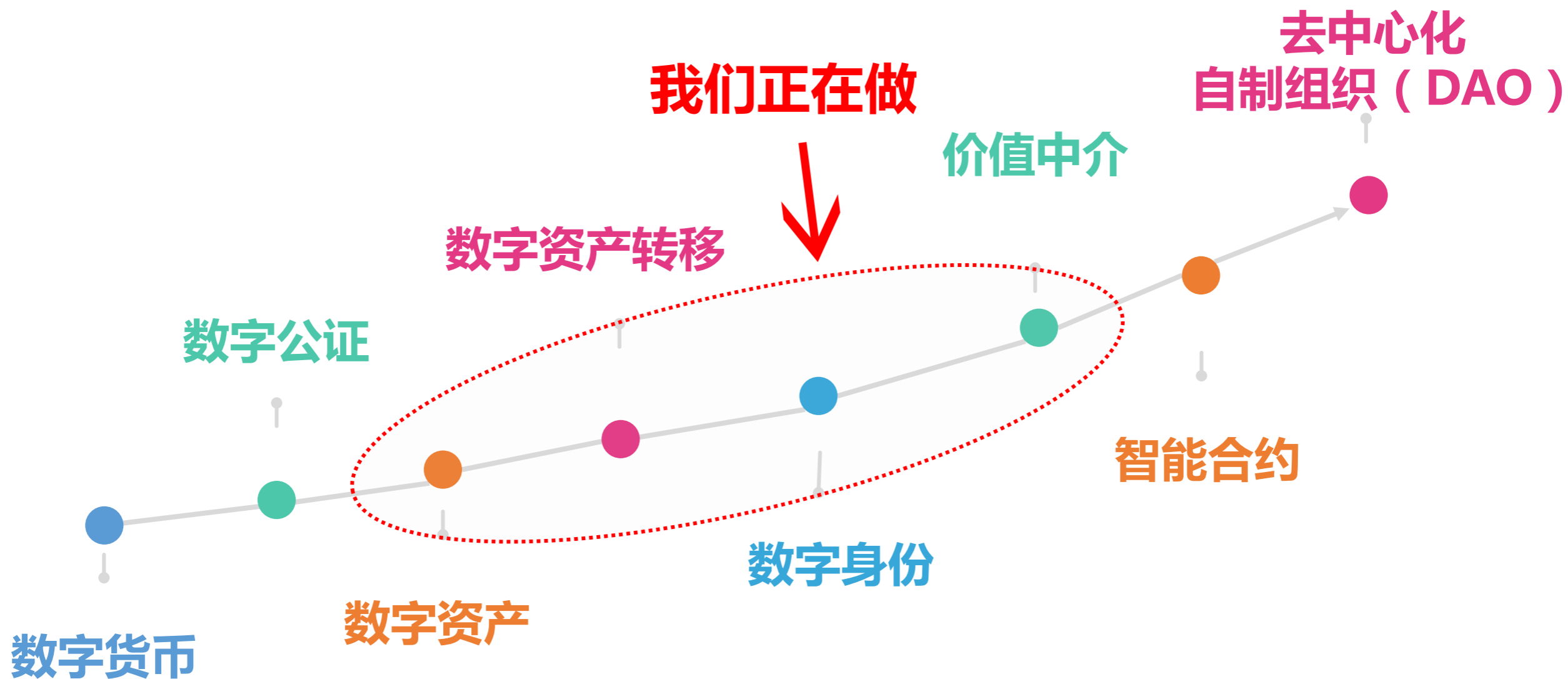
4 账户与存储模型

- UTXO记账和余额记账
- K-V存储与或RDS存储
- 查询接口/交易接口



产品要素

我们正在做



区块链即服务

BaaS 区块链即服务 (Blockchain as a service)

- ✓ 注重业务重塑过程
- ✓ 具有通用性
- ✓ 使用现有区块链
- ✓ 开放的服务

- 1、区块浏览器
- 2、数字货币交易平台
- 3、存证型应用-Factom等
- 4、数字身份型应用-uPort等

BTaaS 区块链技术服务 (Blockchain technology as a service)

- ✓ 注重技术过程
- ✓ 针对具体场景
- ✓ 构建自己的区块链实例
- ✓ 封闭的服务

- 1、各种私有区块链具体应用
- 2、HyperLedger Fabric
- 3、Multichain

以BaaS为基础进行金融创新

将区块链服务BaaS和区块链技术服务BTaaS相结合

BaaS提供新金融的模式以及不可篡改、公开透明的服务（对外）

BTaaS提升企业内部运作效率（对内）

Part 3 公有区块链技术应用——Metaverse元界



元界技术选型与钱包架构



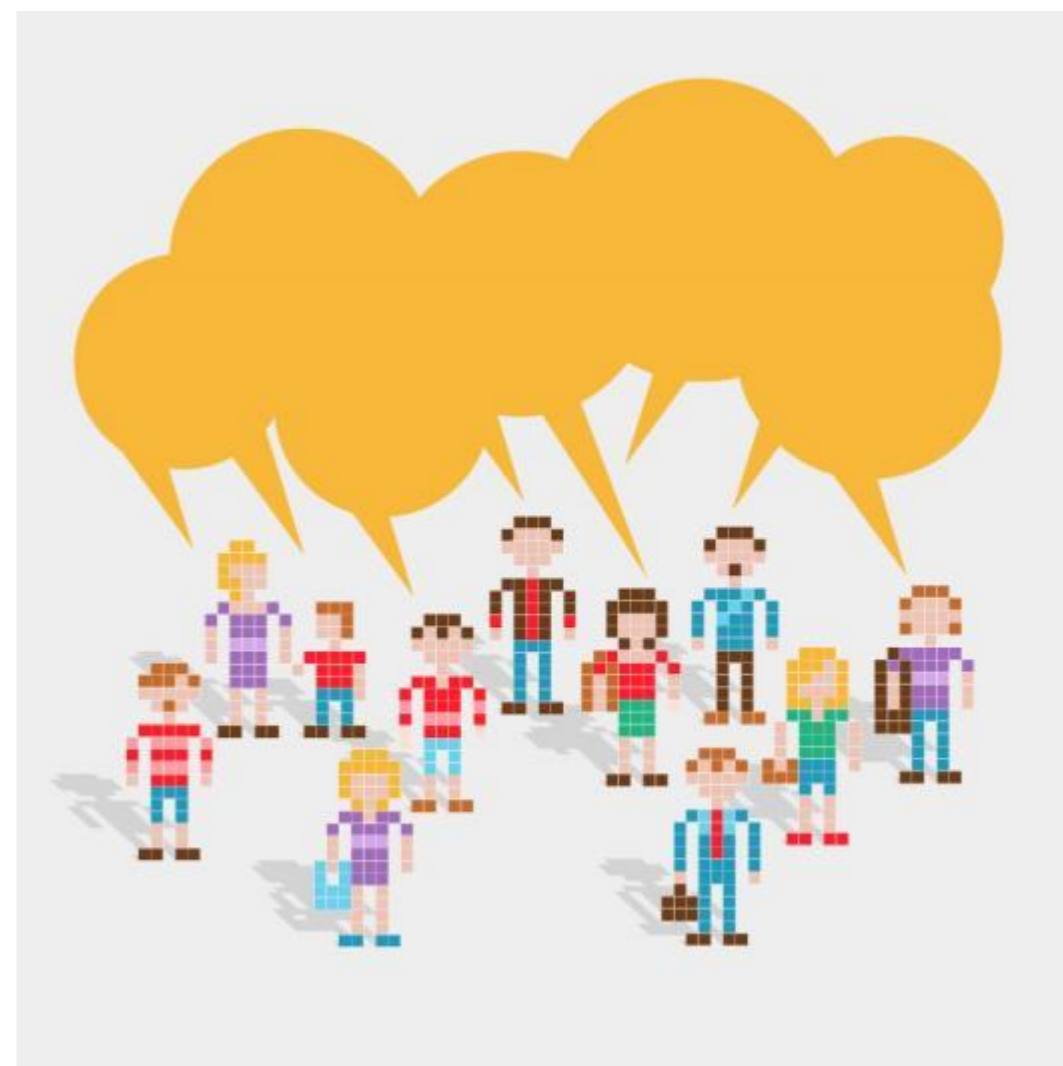
元界实践时遇到的问题



元界的MIPs
(Metaverse Improvement Proposals)



元界的区块链即服务



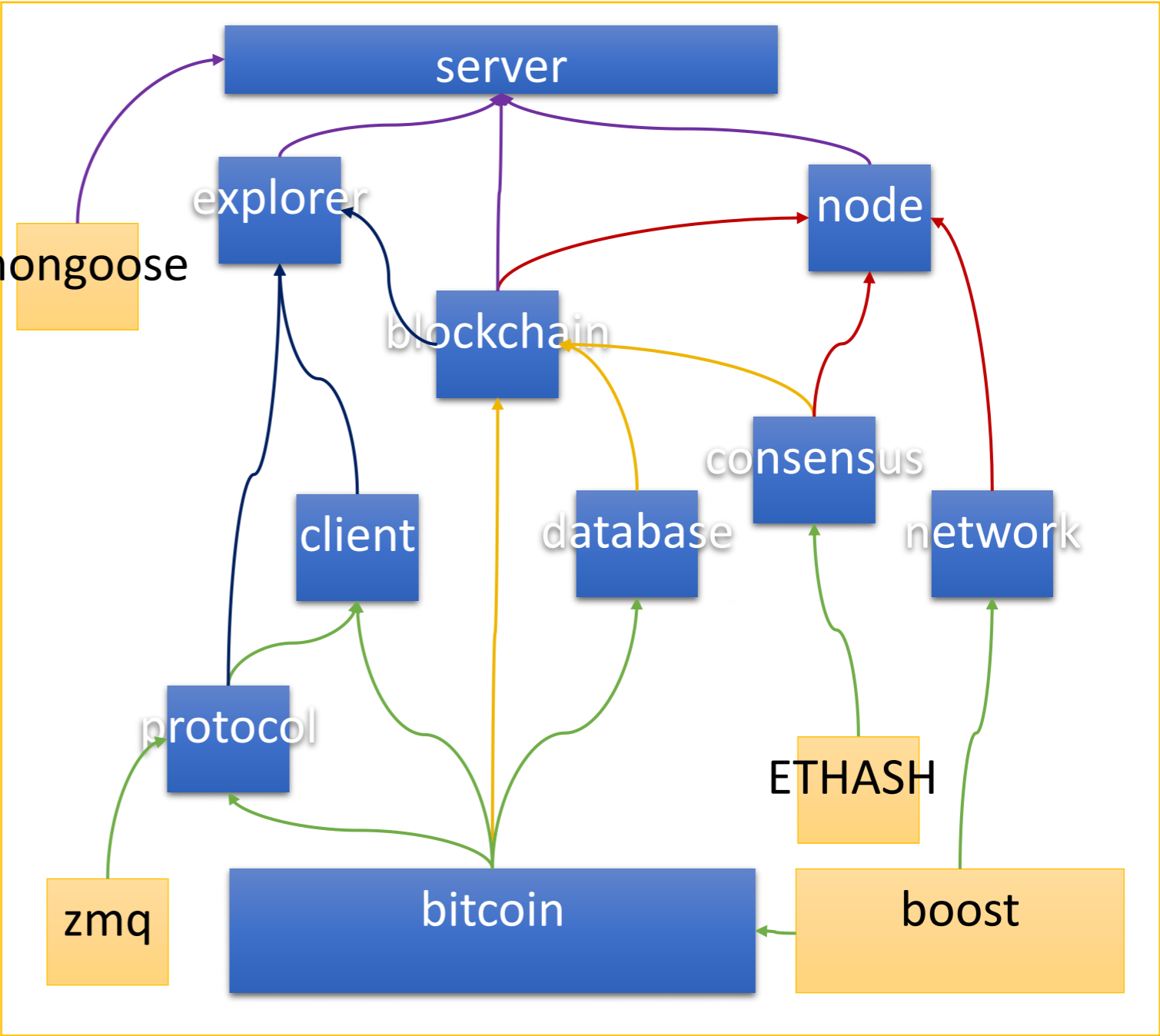
元界技术选型

P2P网络协议
比特币70012版本协议

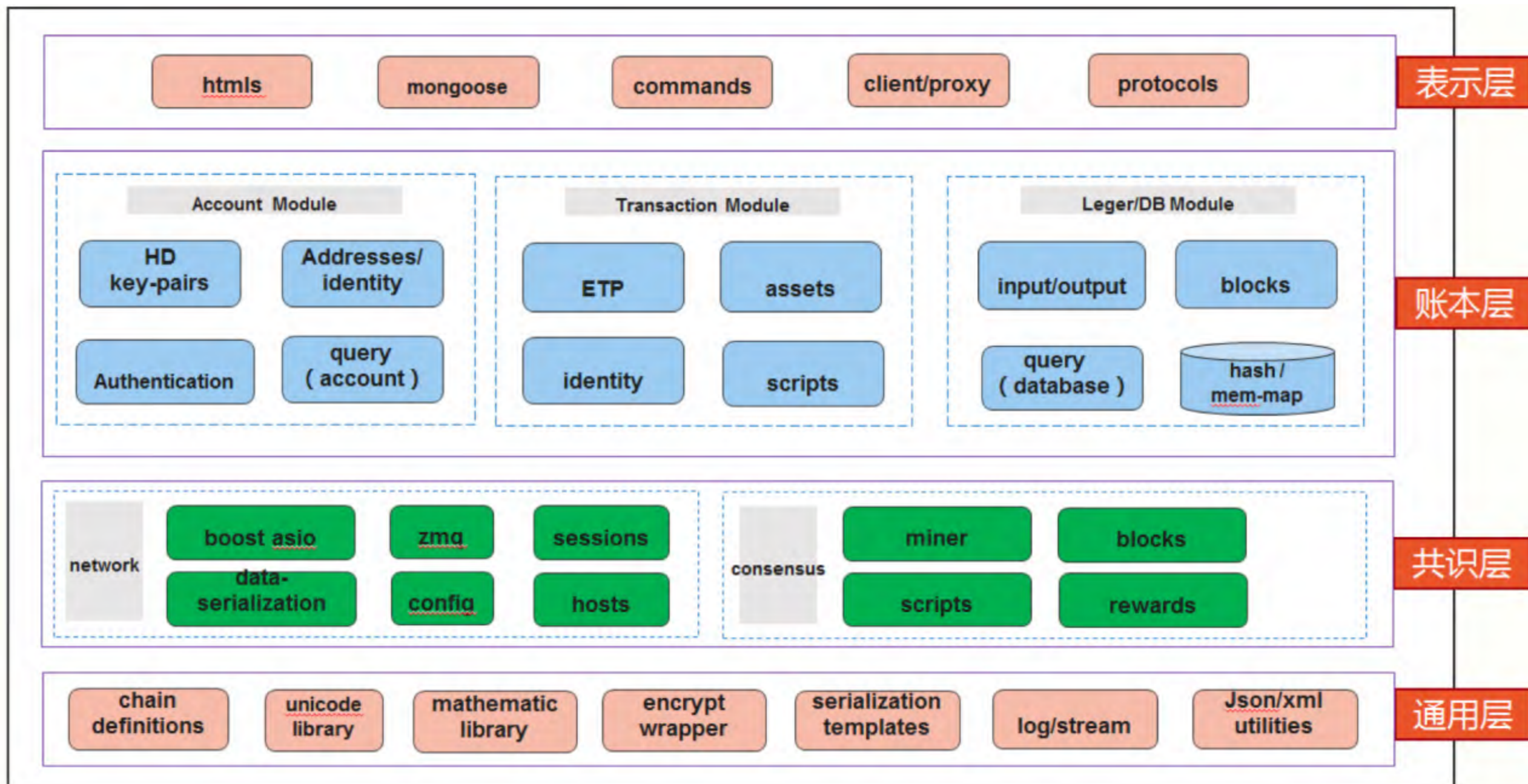
共识算法
ETHASH
(Dagger-Hashimoto算法的改良版本)

加密与签名算法
椭圆曲线ECDSA
(Secp256k1)

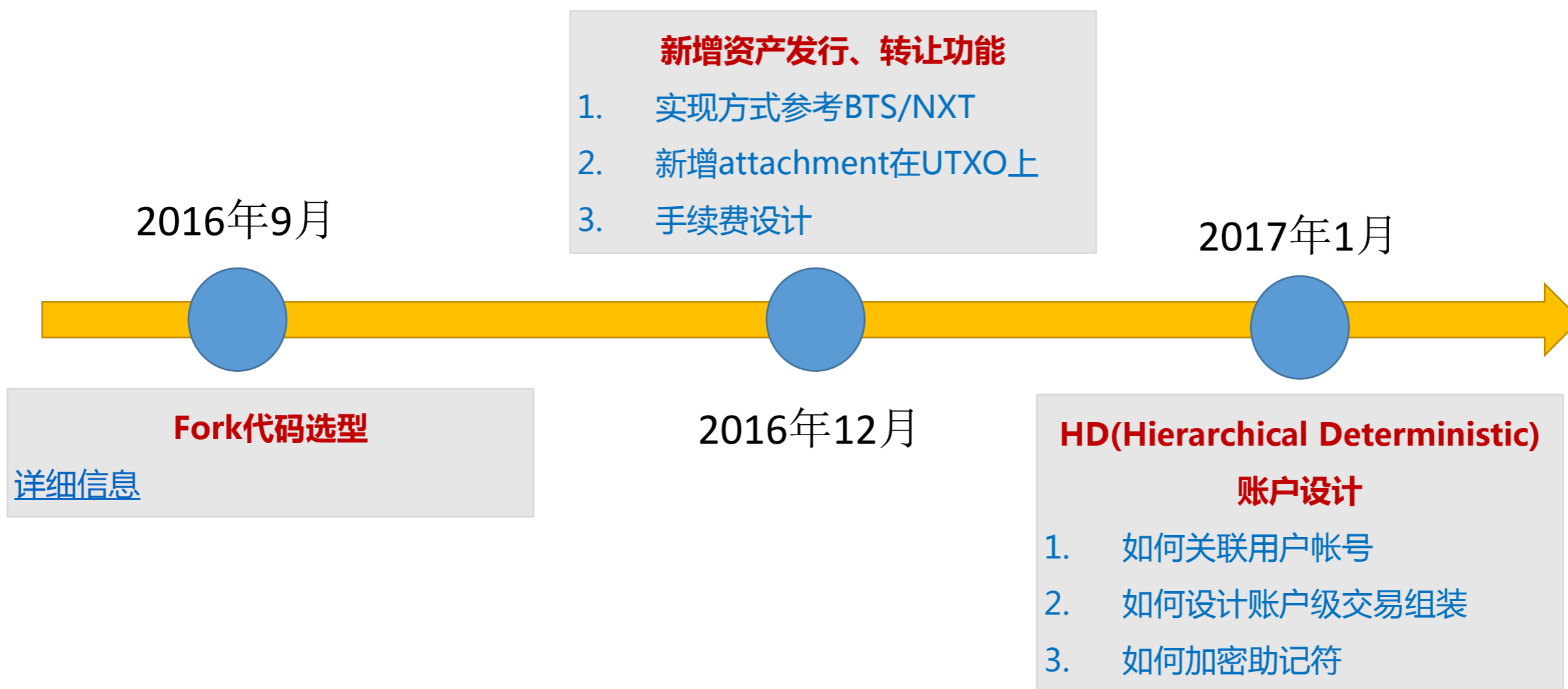
账户与存储模型
UTXO 扩展版本
Memory-map 存储



元界钱包架构



技术实现时遇到的问题

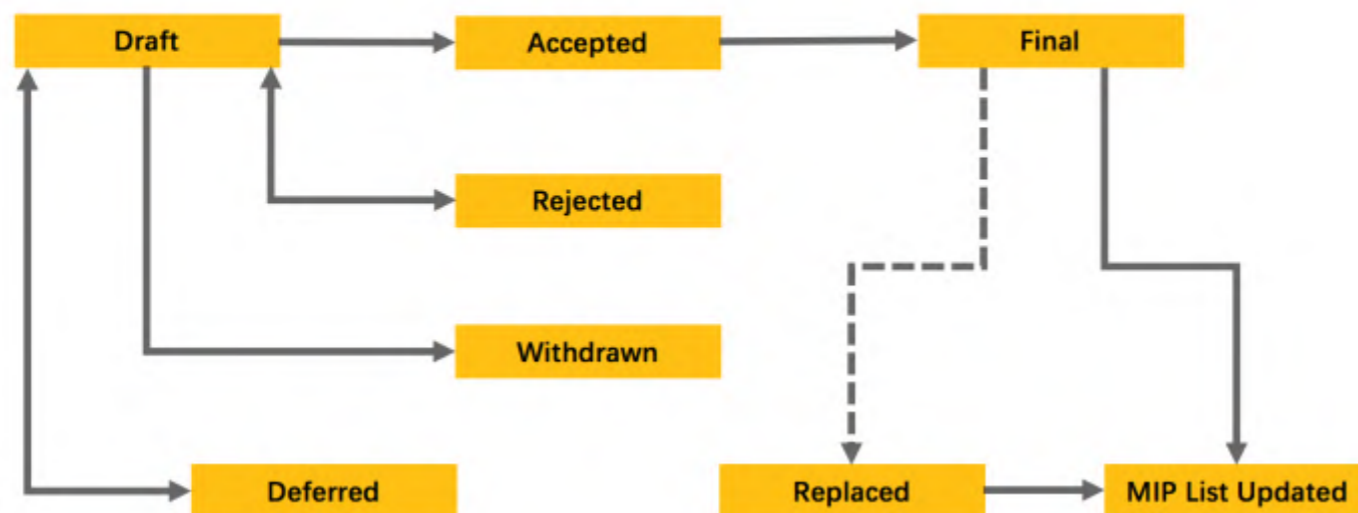


主网运行遇到的问题



元界的MIPs

MIP Process



现已开放的MIP：

- **MIP-001 资产冻结**
- **MIP-002 个人数字身份**

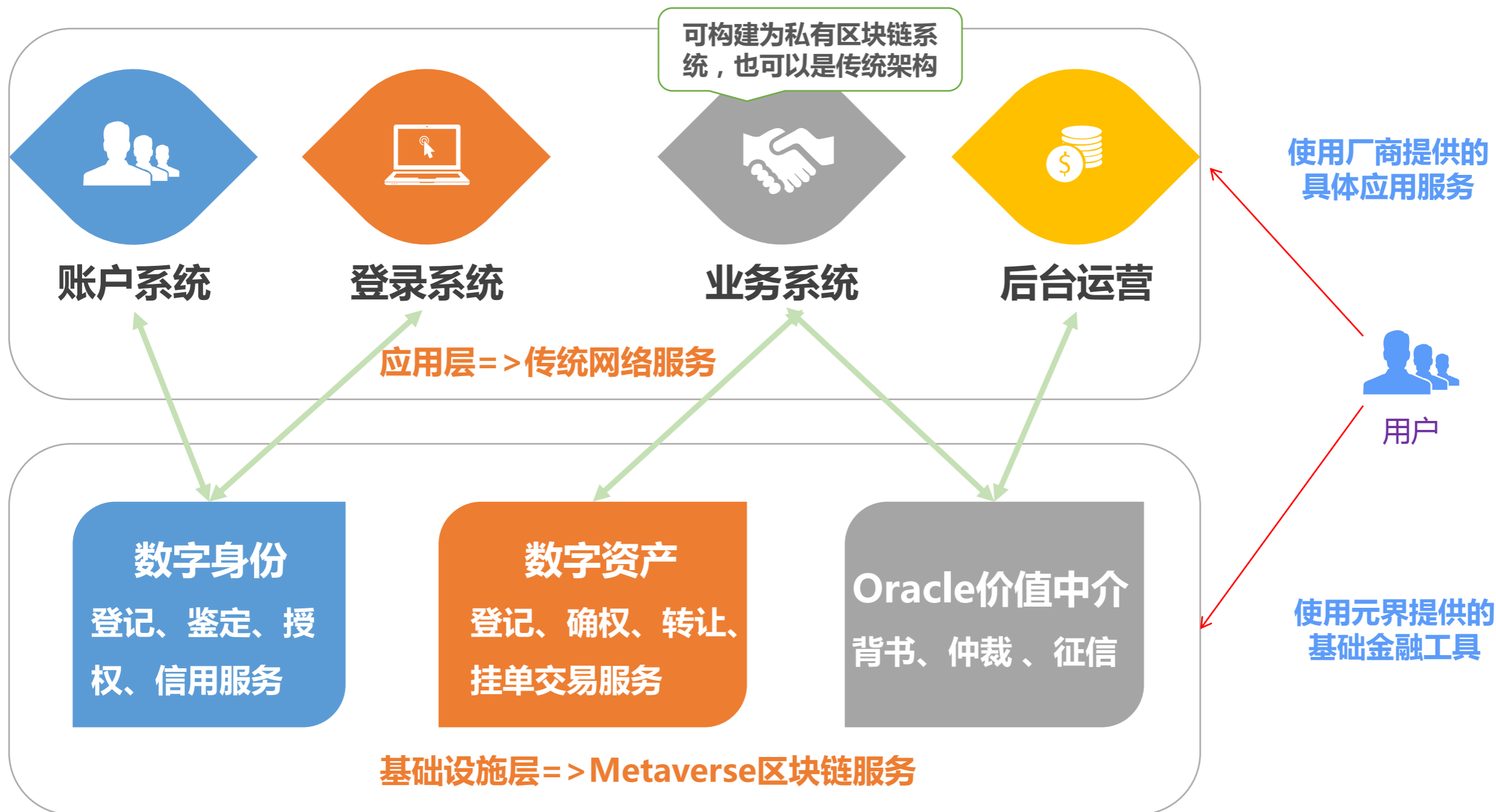
<https://github.com/mvs-org/mips>

- **公链的常青法则-MIP**
(Metaverse Improvement Proposals)
- **杀手级应用-区块链数字身份**

数字身份的难点：

1. 数字身份在区块链上的隐私性问题；
2. 数字身份在授权过程中避免信息泄漏；
3. 身份的多面性以及身份的时效性如何在区块链上体现。

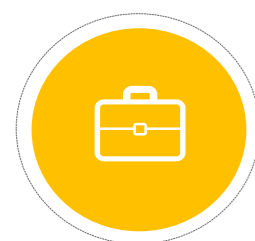
元界的区块链即服务



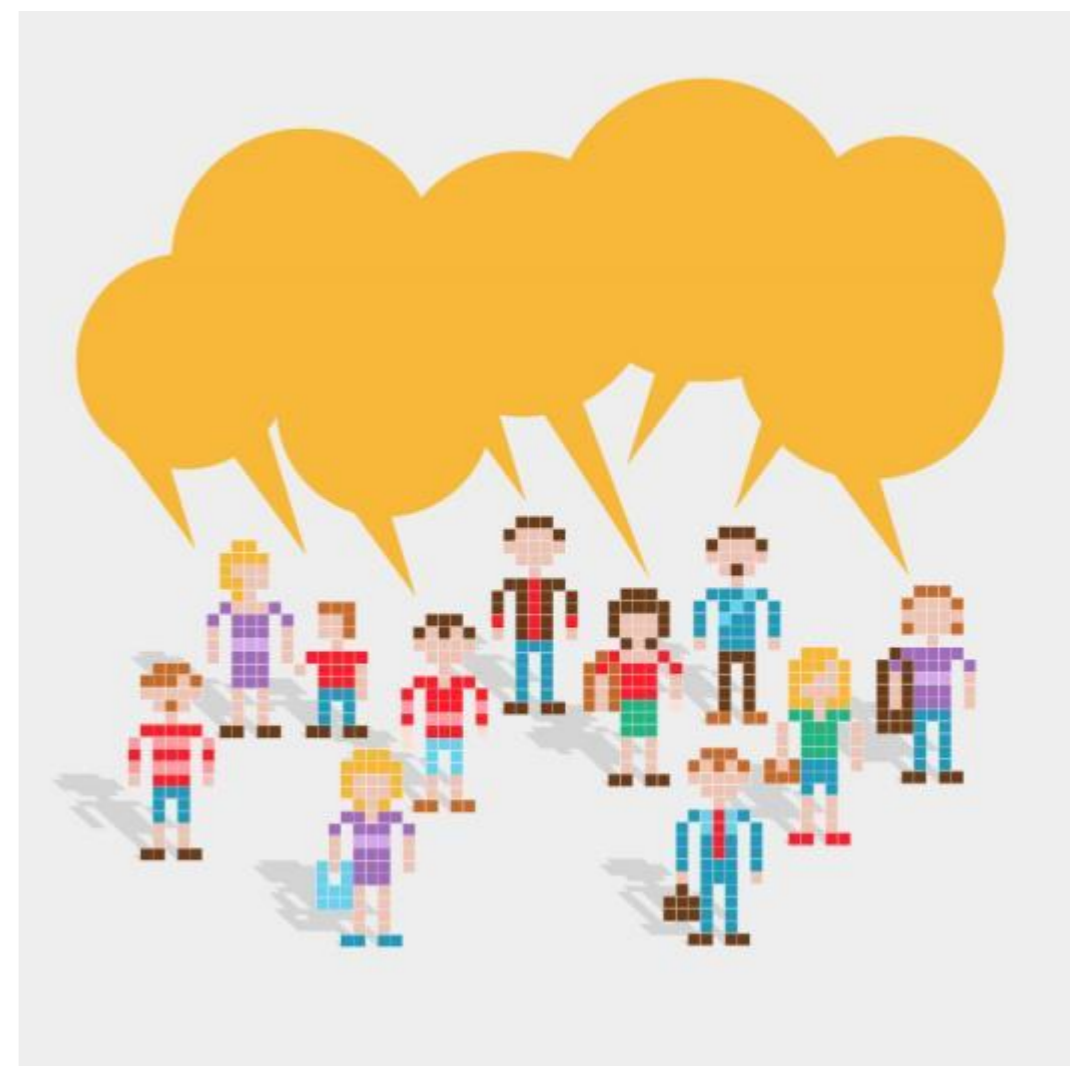
Part 4 公链即服务——未来新架构模式



新业务上链的探索



基于BaaS技术架构演变探索



新业务上链的探索



基于元界区块链，并由实体黄金背书的人工智能资产体系，应用了元界的数字身份体系，结合区块链技术对每一克黄金进行实名确权。



基于元界公链开发的平台，通过将收藏品数字化，将实体资产与其在区块链的数字化资产产生关联，为这些数字权益提供转让、借贷等价值流通渠道。

基于BaaS技术架构演变探索

1

微服务+区块链服务BaaS=关键数据永不可篡改

2

个人数字银行服务——提供各种基础BaaS服务的运营商（可云、可托管）

3

基于离线交易签名与轻支付的移动端产品

4

服务端构建链上金融衍生品基础设施

5

区块链支付加速通道（闪电网络、代理商）



THANK
YOU



<http://viewfin.com>



维优CTO 陈浩

让创新技术推动社会进步

HELP TO BUILD A BETTER SOCIETY WITH
INNOVATIVE TECHNOLOGIES

Geekbang >

极客邦科技

InfoQ
ueue

专注中高端技术人员的技术媒体



EGO EXTRA GEEKS' ORGANIZATION
NETWORKS

高端技术人员学习型社交平台



StuQ
ueue

斯达克学院

实践驱动的 IT 教育平台

