

互金行业区块链评估及应用实践

2.0.20170606

刘胜 首席架构师

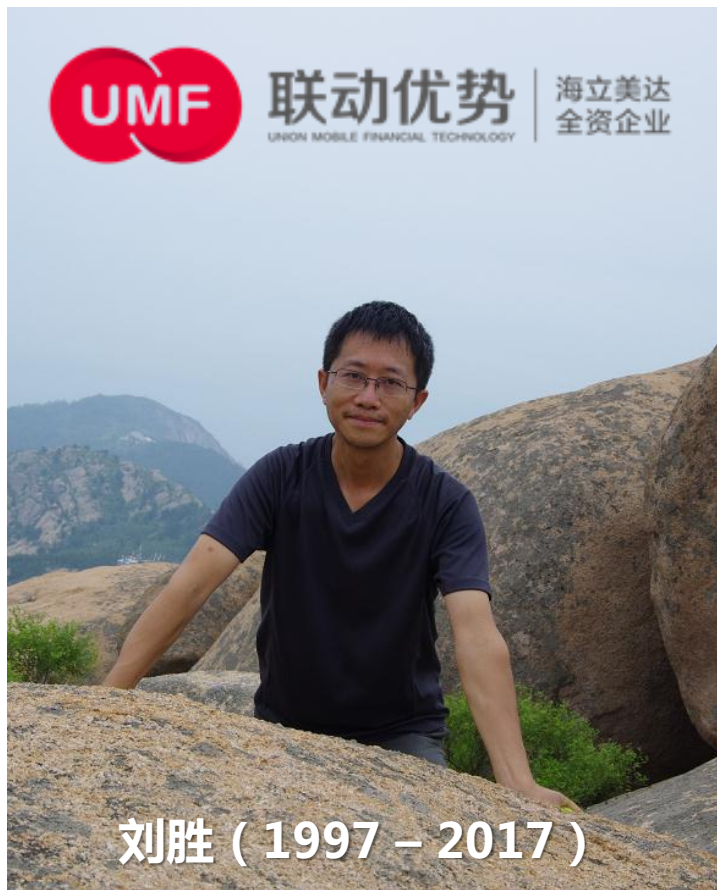
联动优势科技有限公司 (海立美达 002537)

个人介绍



华章科技

IT大咖说
知识分享平台



刘胜 (1997 – 2017)

1.行业

- 电信行业
- CA
- 电子商务
- 移动支付 (14y)

2.经历

程序员
系统分析员
资深系统分析师
首席架构师
(3/35+)发明家
专家 / 科学家

3.协会

- 中国互金协会
 - 区块链工作组
- 支付清算协会
 - 分布式架构组
 - 数字货币研究组

4.其他

《支付清算行业分布式系统架构研究与设计参考》
《可信区块链标准》
北京市科学技术奖三等奖

...

1

区块链概念和现状

2

互金行业区块链的评估

3

互金行业区块链应用

区块链概念渐近明晰



华章科技

IT大咖说
知识分享平台

区块链是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。

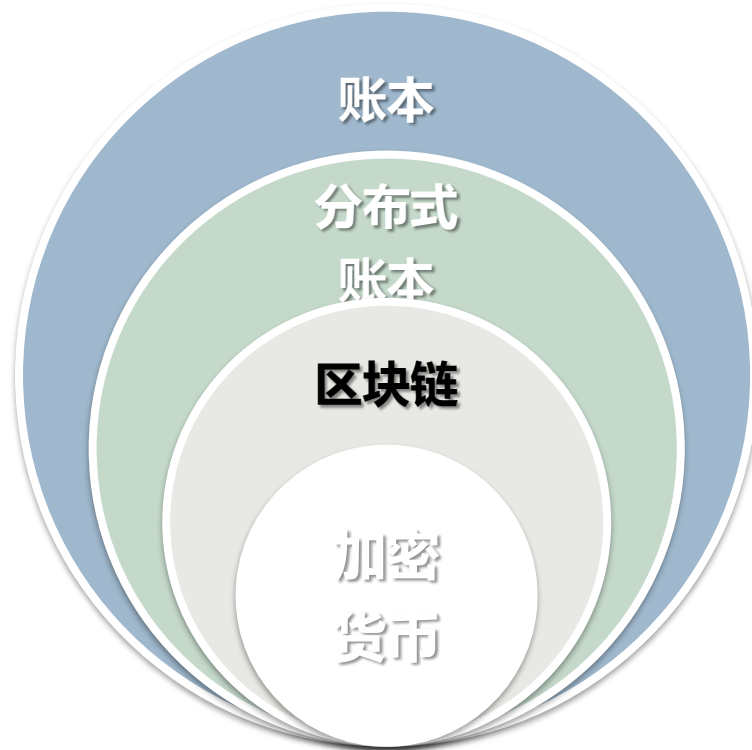
1

2

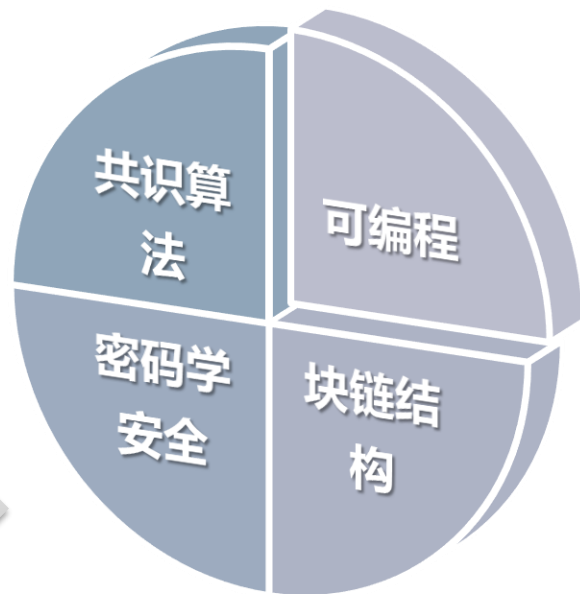
3

4

5



- 1.去中心化
- 2.公开透明 → 信任效果
- 3.原生货币
- 4.可靠 → 可信
- 5.数据库 → 成本
- 6.智能合约 → 可编程



Trust ~~Machine~~ Connector
Internet of ~~Value~~ Trust

加快信任的传递
降低建立信任体系的成本

区块链

+

?

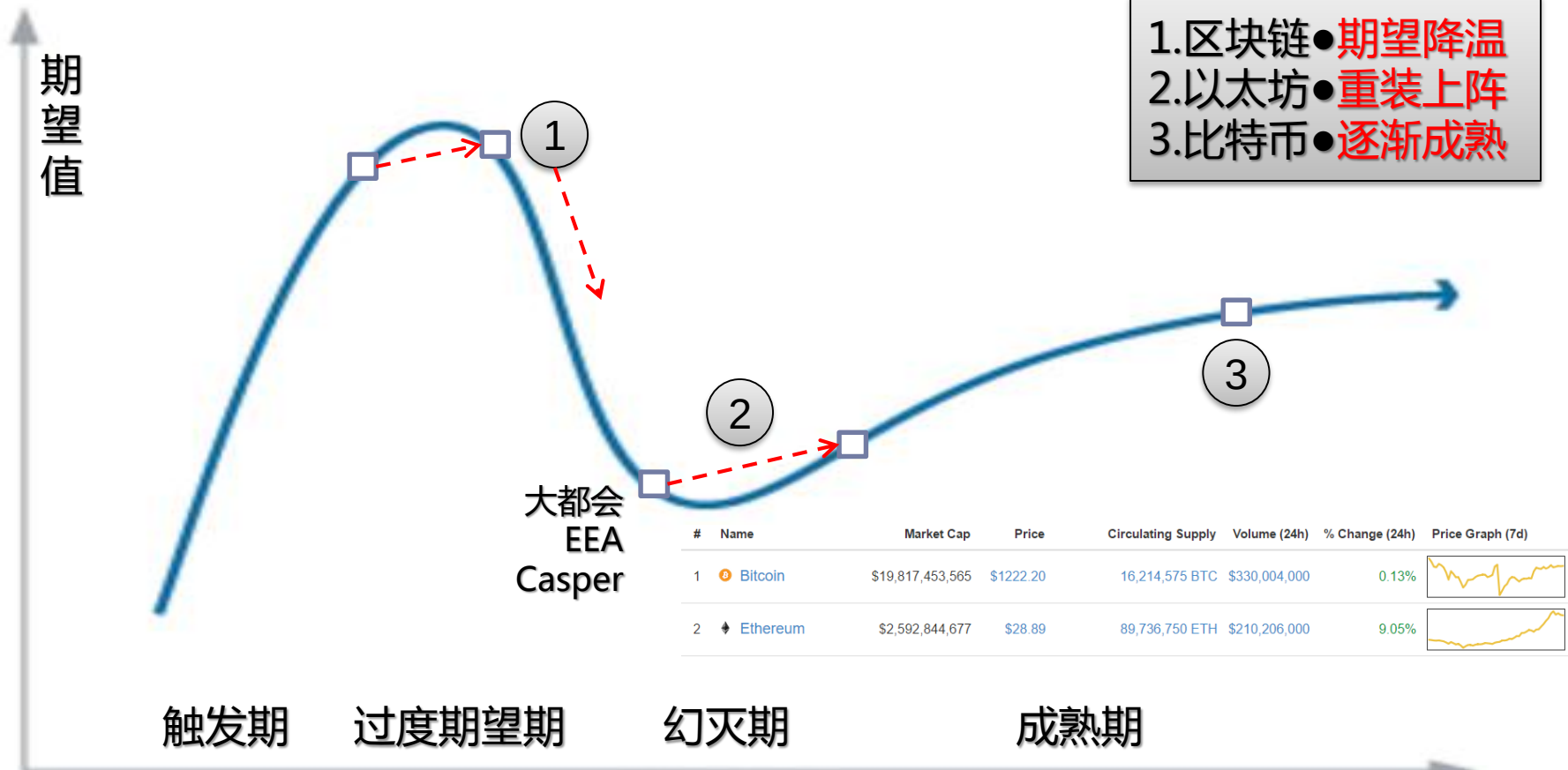
金融
能源
供应链
...

区块链正进入幻灭期



华章科技

IT大咖说
知识分享平台

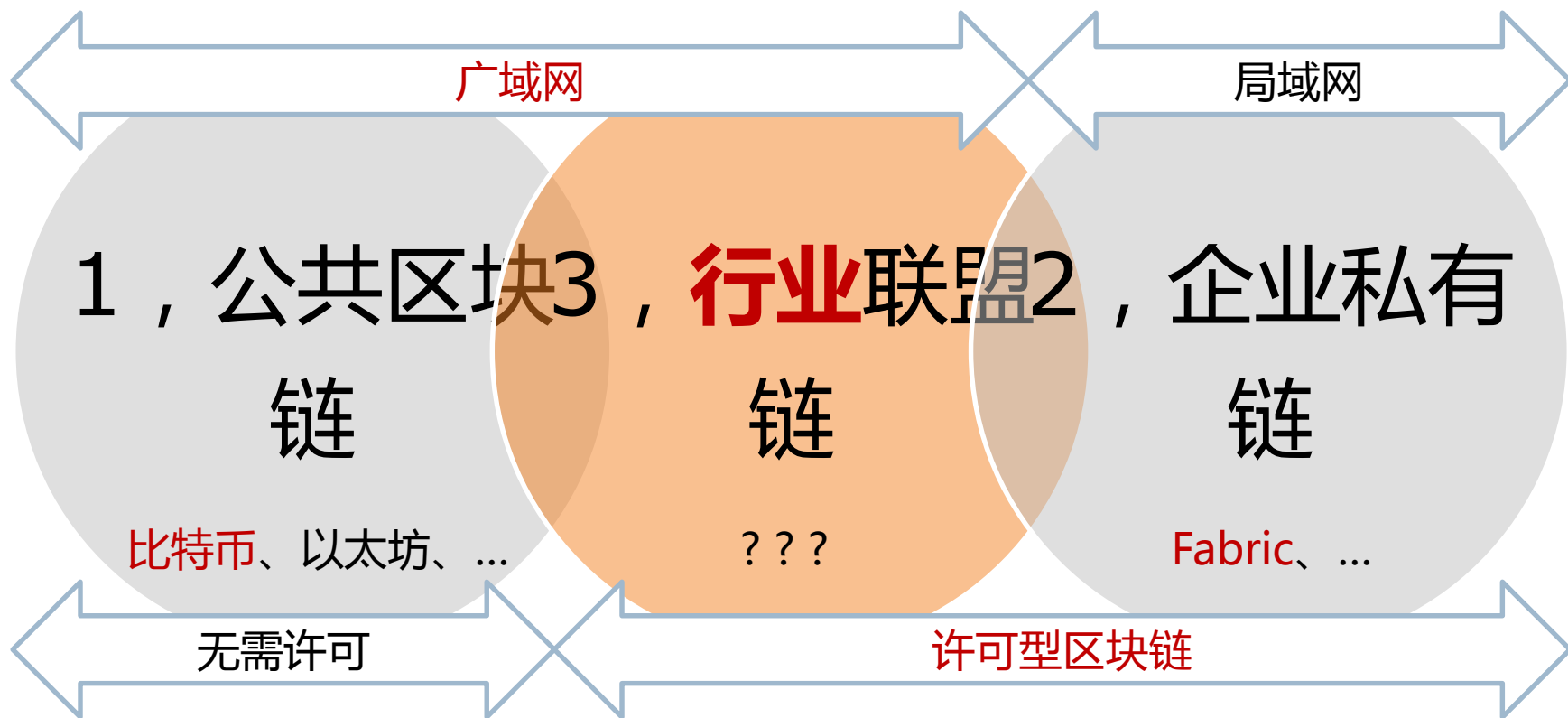


区块链并非成熟技术



华章科技

IT大咖说
知识分享平台



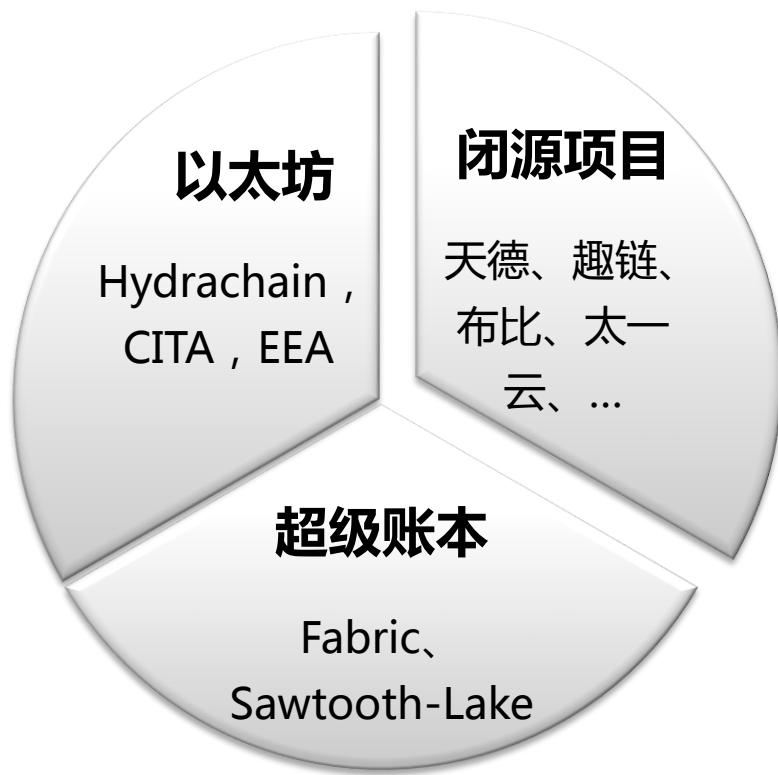
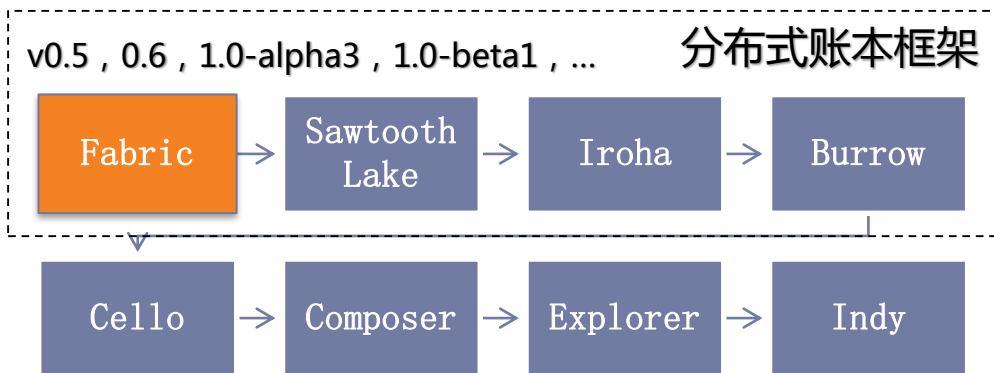
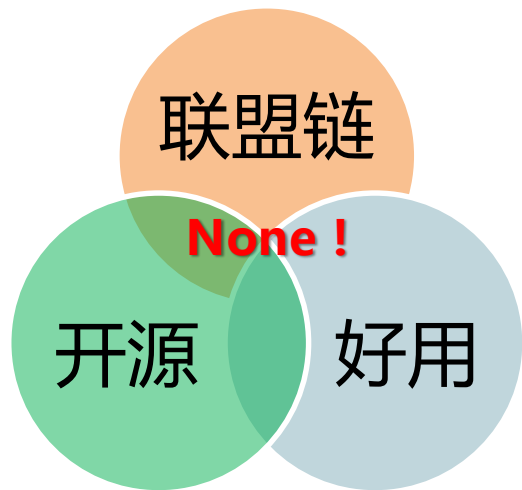
“公共区块链**不**可作为金融机构的解决方案”——R3研究报告

行业联盟链尤其不成熟



华章科技

IT大咖说
知识分享平台



链接：<https://github.com/hyperledger>

1

区块链概念和现状

2

互金行业区块链的评估

3

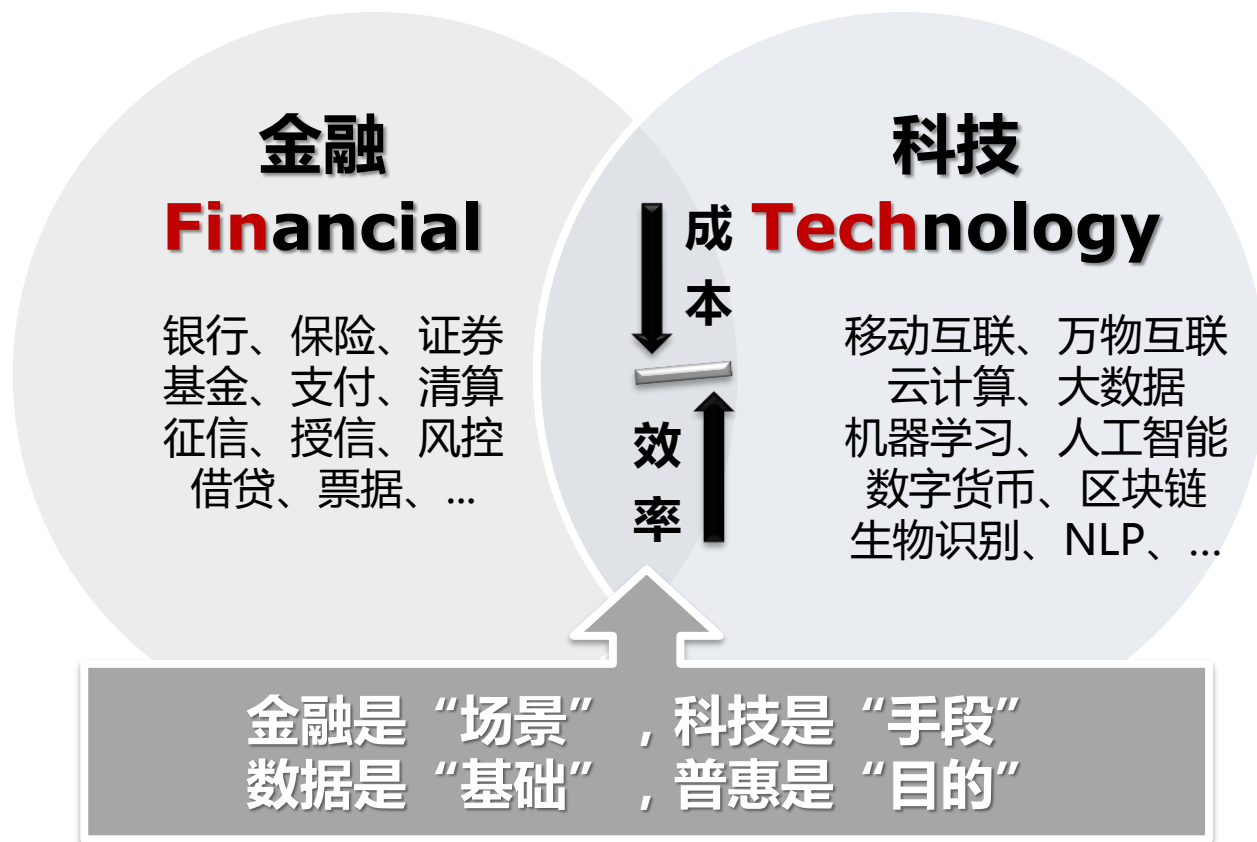
互金行业区块链应用

互金行业的业务复杂多样



华章科技

IT大咖说
知识分享平台



互金业务

P2P网贷、
第三方支付、移动支付
互联网银行、资产管理
互联网保险、网络互助
互联网券商、网络众筹
互联网基金销售
智能投顾、智能证券
大数据征信
供应链金融、保理
个人信用管理
在线投资社交
金融产品搜索
在线金融教育
...

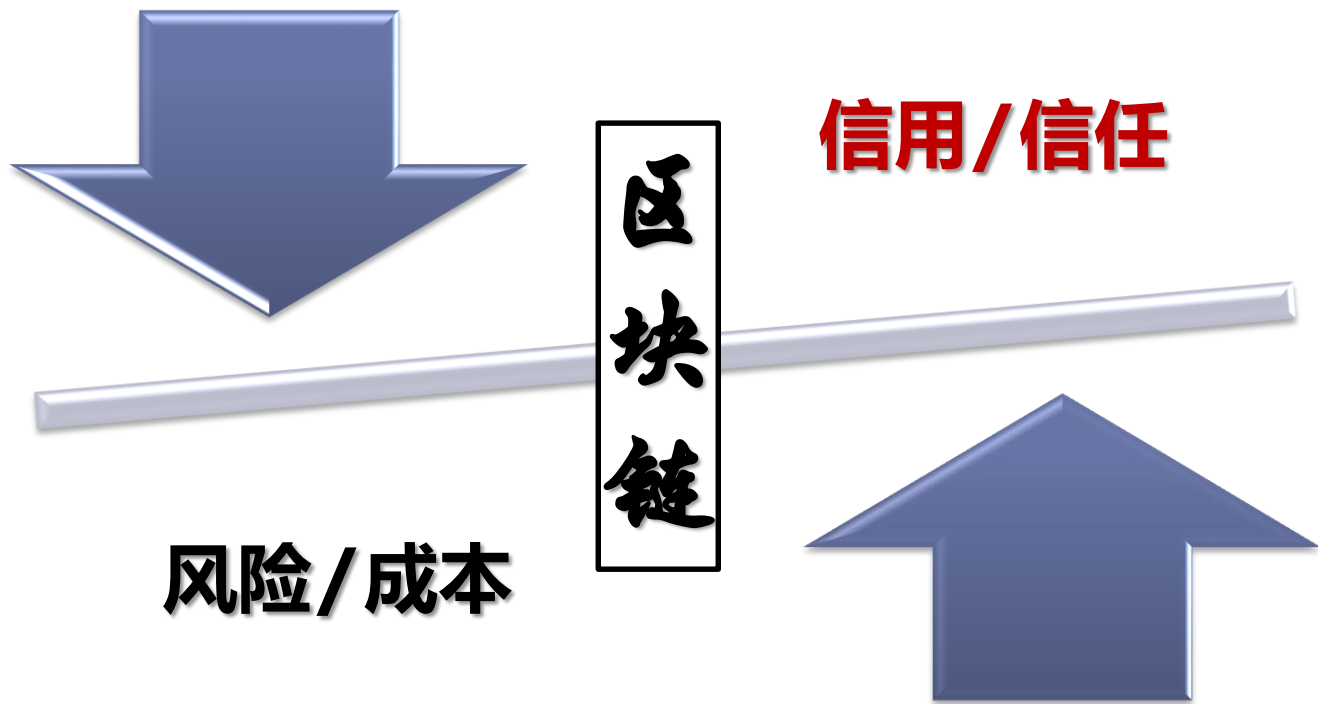
互金行业本质是还是金融



华章科技

IT大咖说
知识分享平台

金融的核心是跨时间、跨空间的价值交换！
——《金融的逻辑》，耶鲁大学教授陈志武



特点

- 机构多，成员复杂
- 成员不固定
- 互不信任
- 强监管
- 网络环境差异大
- 业务规模差异大
- 技术能力差异大

需求点

- 节点多，许可性
- P2P动态组网
- 隐私保护，可验证
- 监管透明
- 跨机房/地域/运营商
- 横向可扩展性
- 自建 & 托管

测评点

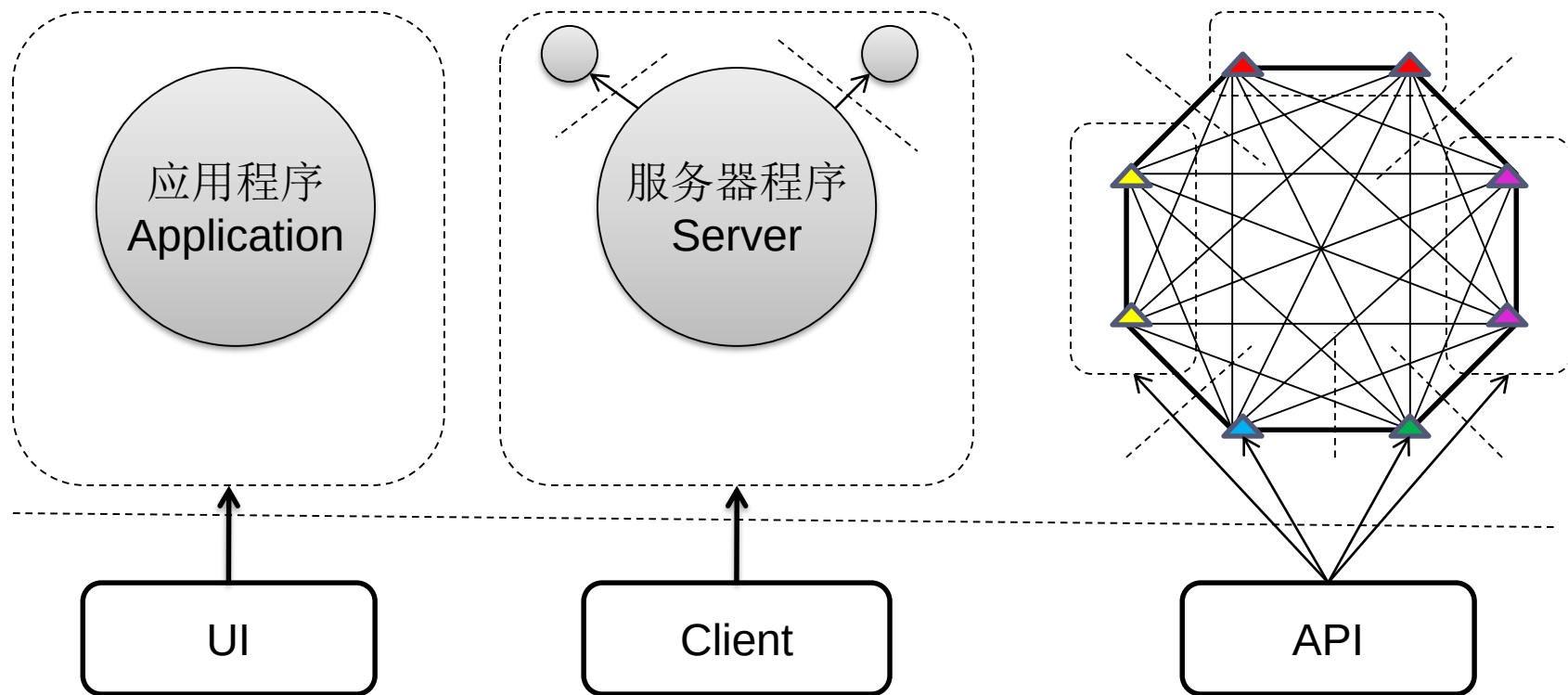
- 节点数（5 | 31 | 101+）
- 动态加入和退出
- 隐私机制，拜占庭容错
- 监管机制
- 网络抖动、闪断、丢包
- 业务扩容、数据扩容
- 快速搭建、升级、迁移

区块链测试难点1：边界模糊



华章科技

IT大咖说
知识分享平台



区块链测试难点2：故障复杂



华章科技

IT大咖说
知识分享平台

故障类型	算法
宕机故障 (Crash Failure)	主副本 , 2PC, 3PC
宕机-恢复故障 / 丢消息 (Crash-Recovery Failure)	Paxos , Raft , ...
拜占庭故障 (Byzantine Failure)	• PBFT , Q/U , Zyzzyva , ... • PoW、PoS、DPoS、...

其他考虑因素		
通信模式	同步	异步
消息认证	认证 / 不可篡改	非认证

FLP不可能性
(结论/定律)

Lamport 结论

区块链测试难点3：类型多样



华章科技

IT大咖说
知识分享平台

区块链类型	公有链	联盟链	私有链
治理模式	无	多机构	单机构
用户身份	无许可	许可	
	未指定，可能包含恶意成员	指定，可靠成员组成	
共识算法	PoW/PoS/DPoS 等	PBFT/Zyzyva 等	
	多块确认 耗电量 大	立即确认 简单/快速/耗电量小	
交易处理时间	长(如：10 min)	短(如：几秒)	
场景	虚拟货币等	银行转账，证券交易等业务网络	
案例	比特币、以太坊等	Ripple、超级账本等	

一般性测试评估的32项共性



华章科技

IT大咖说
知识分享平台

分类	类别	评估项 (20)
质量	性能	吞吐量
		网络延时
		区块确认
		数据访问
	可交互性	开放接口
		跨链接口
		吞吐量
	可扩展性	网络延时
		容量
		节点数
	可靠性	成熟度
		可用性
		容错性
		可恢复性
	安全性	保密性
		完整性
		不可抵赖性
		可验证性
	可移植性	适配性
		易替换性

分类	类别	评估项 (5)
运维	可维护性	模块化
		可重用性
		可分析性
		可修改性
		可测试性

分类	类别	评估项 (7)
成本	研发	区块链底层研发
		子系统研发
	实施 (商业化)	硬件成本
		软件成本
		系统实施成本
	运维	运营成本
		维护成本

区块链测试评估的6大层面



华章科技

IT大咖说
知识分享平台

数据层：结构和存储

- 内容：未确认~/已确认~
- 结构：块头/块体/交易/...
- 存储：内存/文件/K-V/DB

网络层

- 通讯协议（如P2P）
- 传播机制（广播/同步）
- 动态节点（新增/退出）
- 网络环境（局域网|广域网）

密码学安全

- 哈希散列，数字签名/验签，
- 国密，CA，私钥保护，...
- 隐私保护（环签名|盲签名|同态加密）

共识层

- 符合性
- 正确性
- 一致性

合约层

- 合约语言，图灵完备性
- 合约执行，可终止性，...

应用层：跨链交互

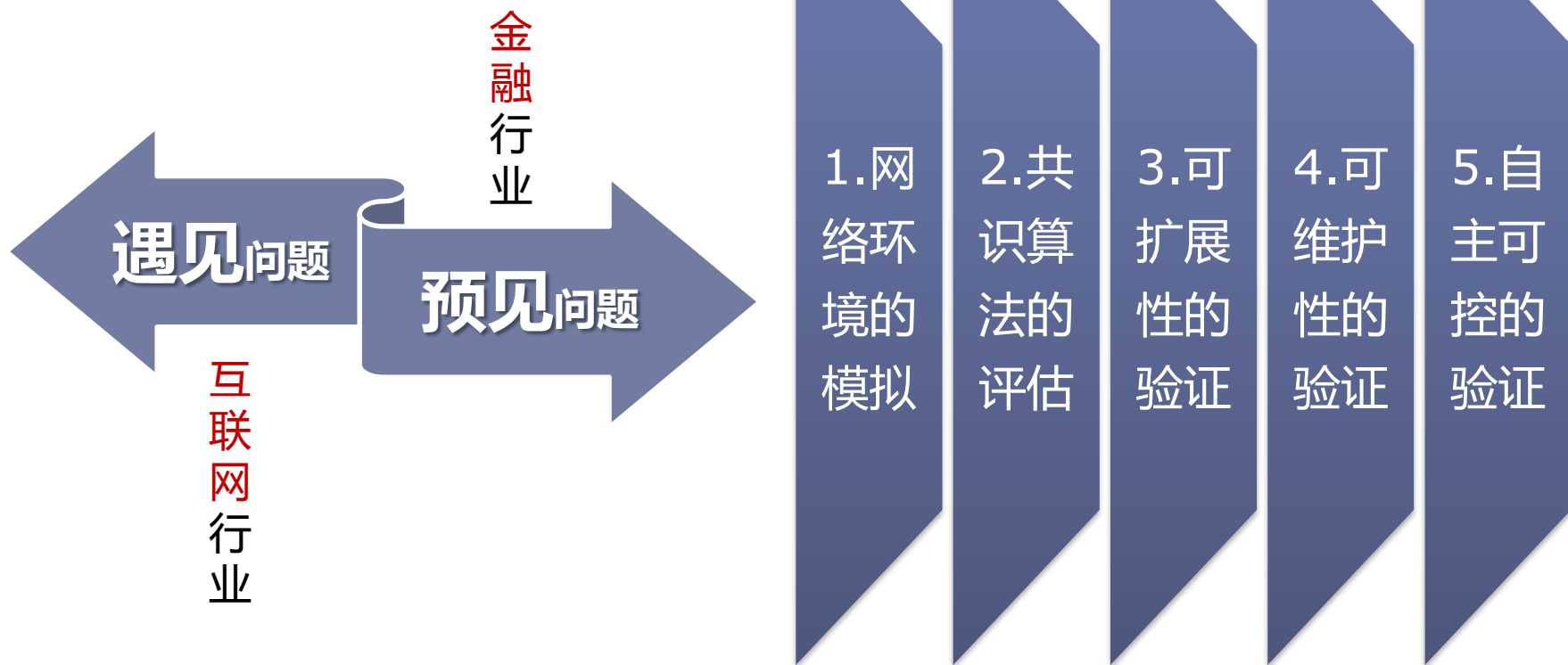
- 目标：资产转移、状态转移
- 方式：公证人、侧链/中继、哈希锁定
- 类型的符合性，正确性

互金行业联盟链的测评重点



华章科技

IT大咖说
知识分享平台



限速

- 命令：/sbin/tc qdisc add dev eth0 root tbf rate 2048kbit latency 50ms burst 2048
- 验证：块落后太多导致不再参与共识？合约执行失败？

乱序

- 命令：/sbin/tc qdisc add dev eth0 root netem delay 1000ms 300ms 30%
- 验证：是否造成节点块不同步？节点不再参与共识？

丢包

- 命令：/sbin/tc qdisc add dev eth0 root netem loss 10%
- 验证：丢交易？节点不再参与同步？节点不再参与同步？

重复

- 命令：/sbin/tc qdisc add dev eth0 root netem duplicate 1%
- 验证：交易存在双花？

损坏

- 命令：/sbin/tc qdisc add dev eth0 root netem corrupt 0.2%
- 验证：是否丢交易（损坏率0.2%时）？是否不参与共识或不同步块（损坏率5%时）？

共识算法的评估



华章科技

IT大咖说
知识分享平台

非拜占庭容错

- Paxos , 1989-1998
- Raft , 2013
- ISR (kafka)



拜占庭容错

- PBFT , 1999
- Q/U , 2005
- Zyzzyva , 2007



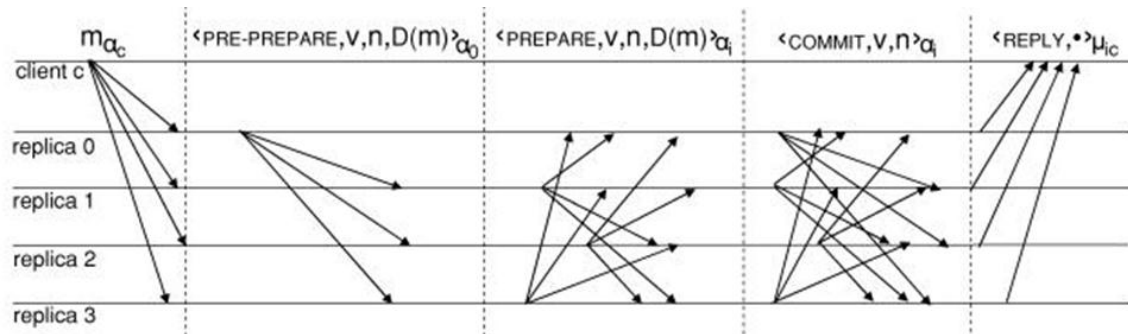
- 1.能够动态组网；
- 2.减少网络交互；

大概率拜占庭容错

- PoW , 1993/1997
- PoS—— ?
- DPoS—— ?

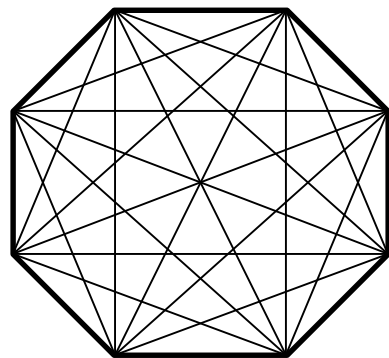


- 3.抵御矿池攻击；
- 4.防范投票失效；



PBFT优点：确定性/终局性

PBFT缺点：通信交互频繁，对网络要求高！



$$N \times (N - 1) / 2$$

数据容量

- 区块大小
- 交易大小
- 出块频率
(确认时间)

业务吞吐量

- 区块大小
- 交易大小
- 出块频率
- 共识算法

网络延时

- 节点分布
- 网络环境
- P2P协议
- ...

节点数

- 数据总容量
- 共识算法

模块化

底层平台

子系统

合约代码

可重用性

底层平台

子系统

合约代码

可分析性

故障探测

性能分析

可修改性

Bug处理

硬分叉

合约代码

可测试性

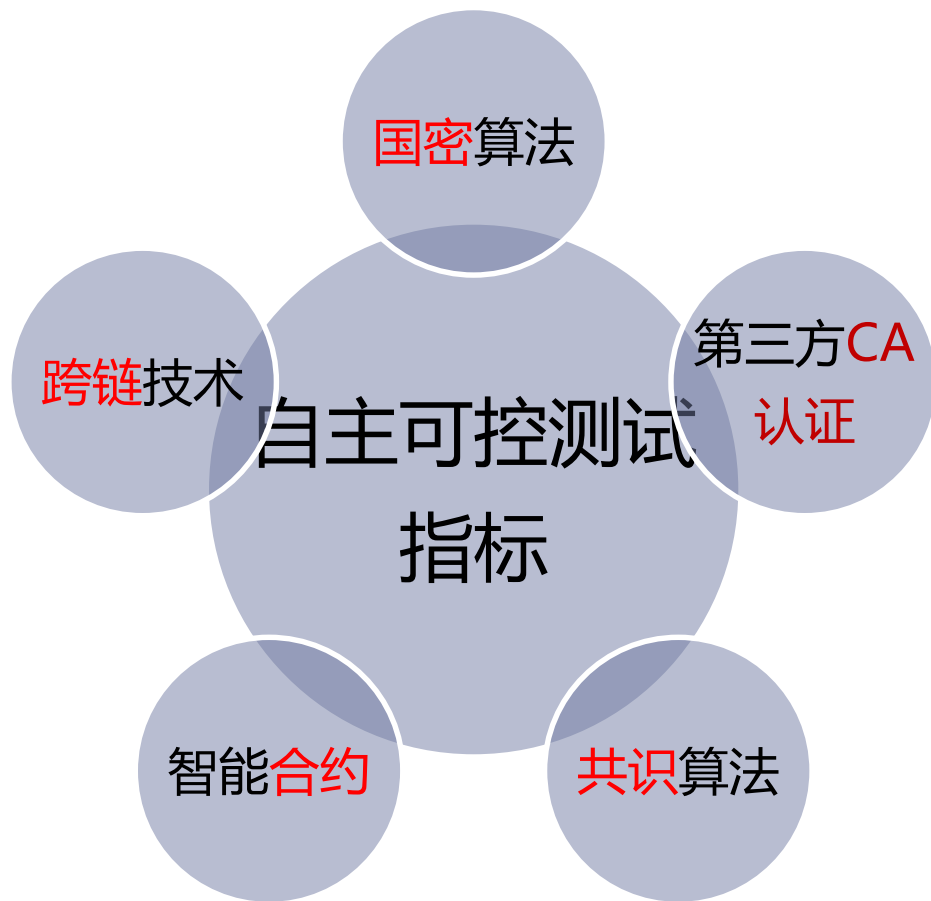
底层平台

容错能力

可扩展性

共识算法

合约代码



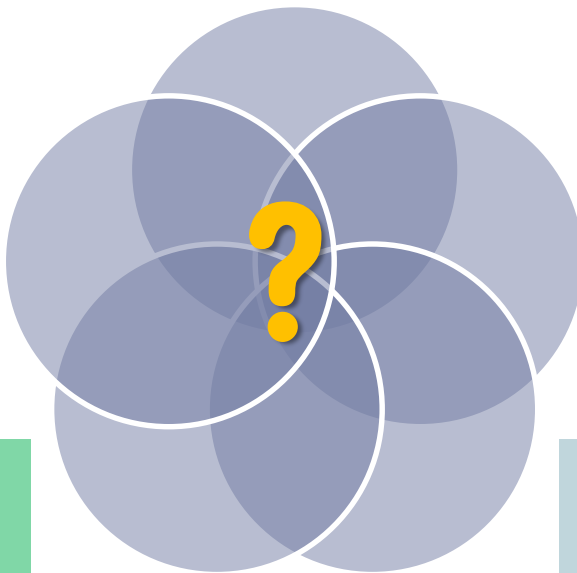
自主可控

可维护

广域网

可扩展

大范围



1

区块链概念和现状

2

互金行业区块链的评估

3

互金行业区块链应用

互金行业经历**爆发性增长**，更加凸显“**信任**”问题。
监管机构启动**强监管模式**，强制要求网贷行业落实“**银行存管**”。

监管机构

- 监管有效性差
- 监管实时性差

存管银行

- 信用背书风险
- 监管成本较高

网贷平台

- 平台信用难建
- 风控成本较高

投资人

- 真实性难验证
- 资金去向存疑

借款人

- 身份核验复杂
- 隐私保护不足

1. 互联网金融举报信息平台
2. 统计监测风险预警平台
3. 互联网金融登记披露服务平台

场景一：风险信息共享



华章科技

IT大咖说
知识分享平台

▶ 已有方案

- | | |
|------------|---------|
| ▶ 模式1：强制上传 | 问题：真实性 |
| ▶ 模式2：路由分发 | 问题：数据沉淀 |
| ▶ 模式3：倡议书 | 问题：真实性 |
| ▶ 模式4：限制范围 | 问题：覆盖性 |

数据**共享**是伪命题！

数据非**占有**，而是**使用**

▶ 新方案：『区块链信息核验**协作**平台』



- 不涉及隐私
- 无泄漏风险

- 平等协作，非数据共享
- 消除信息孤岛
- 多维度，广覆盖

- 历史可追溯
- 评价公正透明
- 信息趋于真实

场景二：金融交易信息存证



华章科技

IT大咖说
知识分享平台



- 金融**标**的信息存证
- 金融**交易**信息存证
- +风险信息存证与共享
- +隐私信息保护与关联

场景三

电子合同存证系统

- 问题：海量电子合同的可靠存储和可信存证
- 方案：第三方的存储、存证、验证

场景四

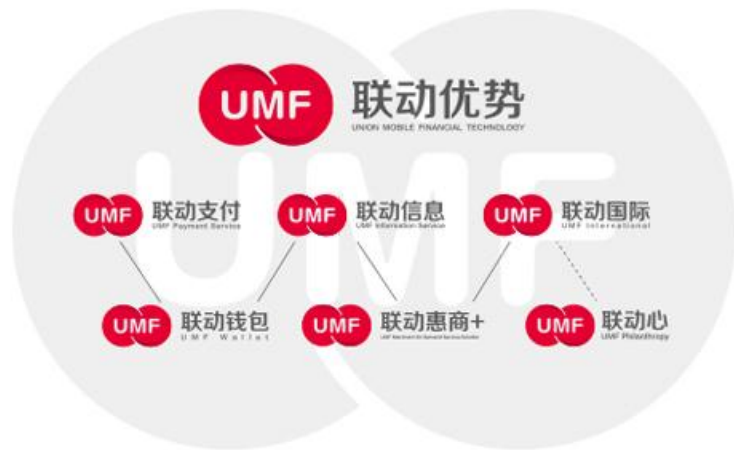
资金存管账户系统

- 问题：在途资金的跟踪，双余额问题
- 方案：类UTXO模型

场景五

跨境结汇+保理

- 问题：多机构间资金流转慢
- 方案：应收款质押，交易信息增信，及时清算



联动优势科技有限公司

2003年由中国移动、中国银联发起成立

联动优势电子商务有限公司

2011年成立，对接第三方支付支付业务

安派国际控股有限公司

2015年成立，对接国际业务

303 Twin Dolphin Drive, 6th Floor, Redwood City,
CA 94065

- 2003年由**中国移动**、**中国银联**发起成立联动优势科技有限公司
- 国内最早涉足移动支付领域的企业，业界公认的移动支付专家
- 中国移动支付领域**唯一**正式合作伙伴
- 领先的移动电子商务及金融信息服务提供商，服务的个人用户**超6亿**。
- 2011年成立全资子公司联动优势电子商务有限公司，构建综合支付平台
- 2011年获得由央行颁发的《**中华人民共和国支付业务许可证**》
- 全国现有**26个**办事处，员工约**800人**，
- 拥有 **U付**、**U信**、**U慧** 3大业务线
- 2014年年交易额过**两千亿**， 年利税逾**3亿元人民币**
- 中国互联网百强**前50名**（ 41/35/27/**36**） - 中国互联网协会和工信部
- 2016年重组获批，成为 **海立美达[002537]** 全资子公司
- 多个**行业协会**的理事单位：中国支付清算协会、中国互金协会， ...
- 多个**区块链联盟**的成员：
 - 中关村区块链产业联盟，
 - 深圳金融区块链联盟，
 - Linux基金会超级账本，
 - 中国互联网金融协会-区块链工作组

Q & A



华章科技

IT大咖说
知识分享平台

谢谢聆听!



谢谢!