China · Beijing

当互联网金融遇到区块链
--成熟的技术也能激发业务变革

邓明

国付宝 CTO

ArchSummit
全 球 架 构 师 峰 会 2016

[北京站]

主办方 Geekbang. 极客邦科技 InfoQ

国付宝介绍

国付宝信息科技有限公司是依托商务部下属单位中国国际电子商务中心发起，与海航集团联手组建，针对企业及个人需求和电子商务的发展，精心打造的国有背景独立第三方支付平台。

2011年12月22日公司正式获得中国人民银行颁发的互联网支付和移动支付业务许可证。2015年1月获基金支付业务许可，2016年5月获跨境人民币支付业务许可。

大纲

区块链的来源及特点

金融领域参考案例分析

互联网金融的区块链创新

基于区块链的比特币(Bitcoin)给了世人一个大惊喜

- 2008年，中本聪在一个密码学邮件群组中发表了文章《比特币：一种点对点的电子现金系统 Bitcoin: A Peer-to-Peer Electronic Cash System》，其中提到了区块链（ Block Chain ）的思想

火币网2016/11/25

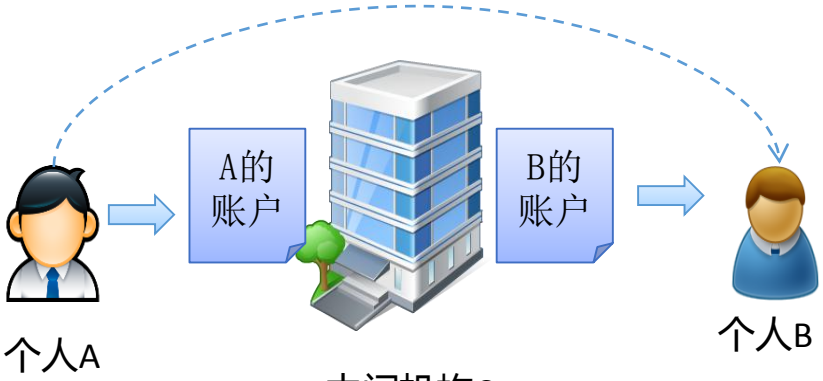
注释：数据来自 bitcoincharts.com

比特币市值突破100亿美元 ，中国交易量超总量九成

----- TechWeb 2016.6

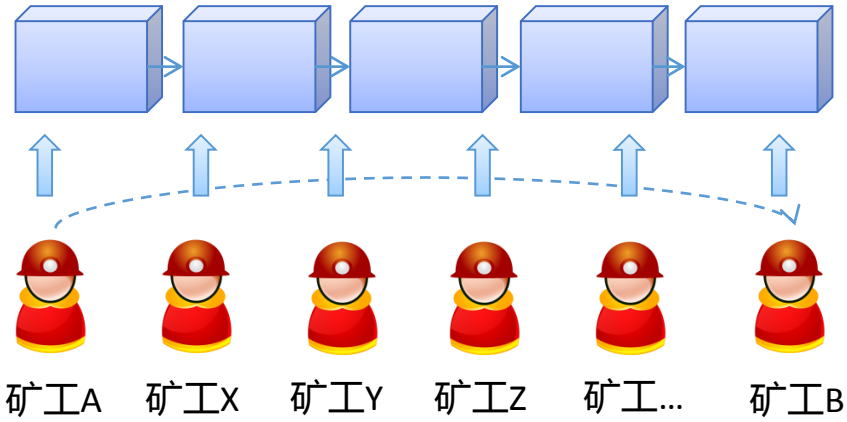
比特币是如何颠覆传统支付流程的

传统的支付流程



- A要把钱转给B
- 需要经过中间机构C
- AB存备付金在C
- AB与C对账

比特币支付流程



- A直接把比特币转给B
- 所有矿工参与记账，通过抢记账权获取比特币
- 矿工自己更新总账

问题：如何避免记假账？如何判断以谁的记录为准？如何避免“双花”？

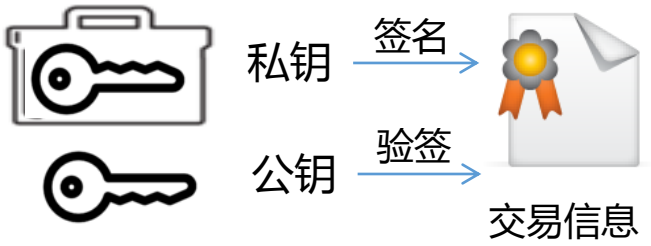
没有实物抵押，也没有政府背书的比特币是怎么做到的？

如何避免记假账？

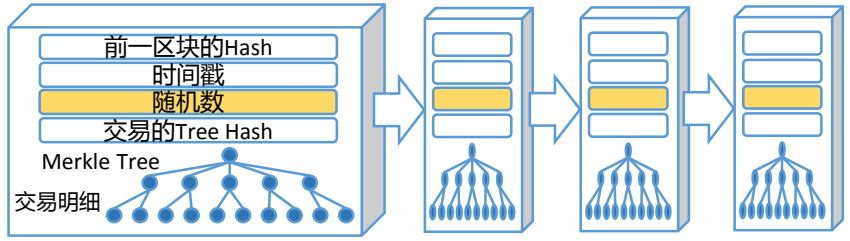
如何判断以谁的记录为准？

如何避免“双花”？

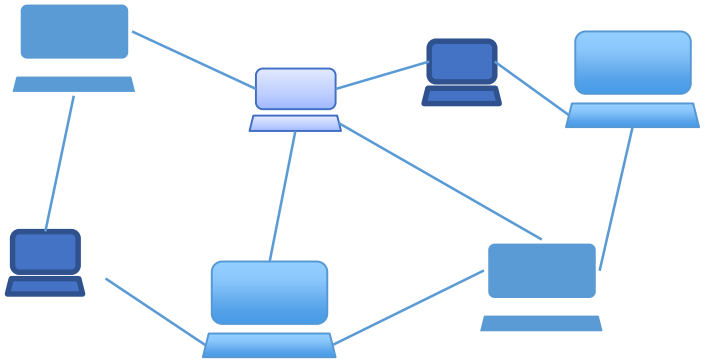
感受一下区块链中多种技术巧妙组合之后的效果



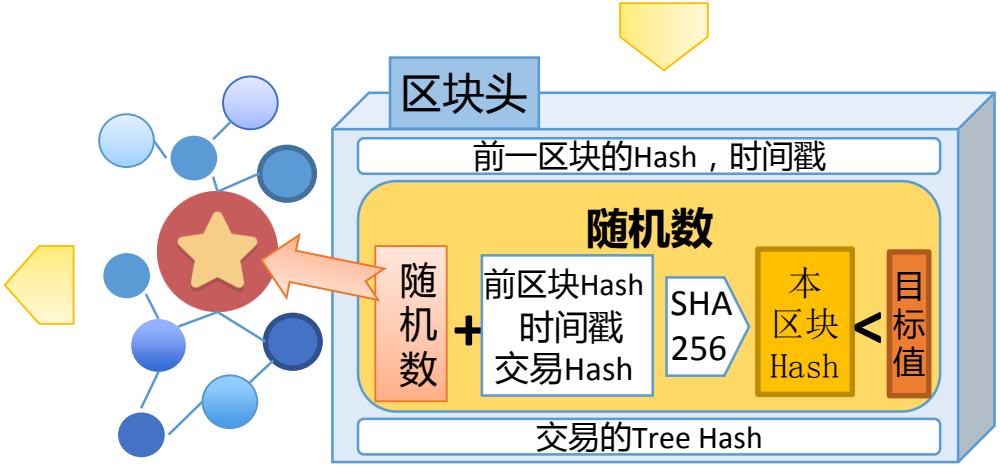
1. 用非对称密钥对交易信息签名，并广播



2. 验证交易，组装区块，并形成区块链结构

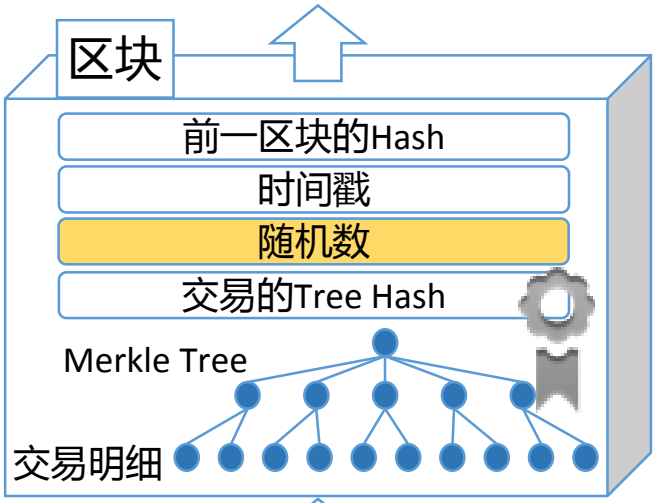


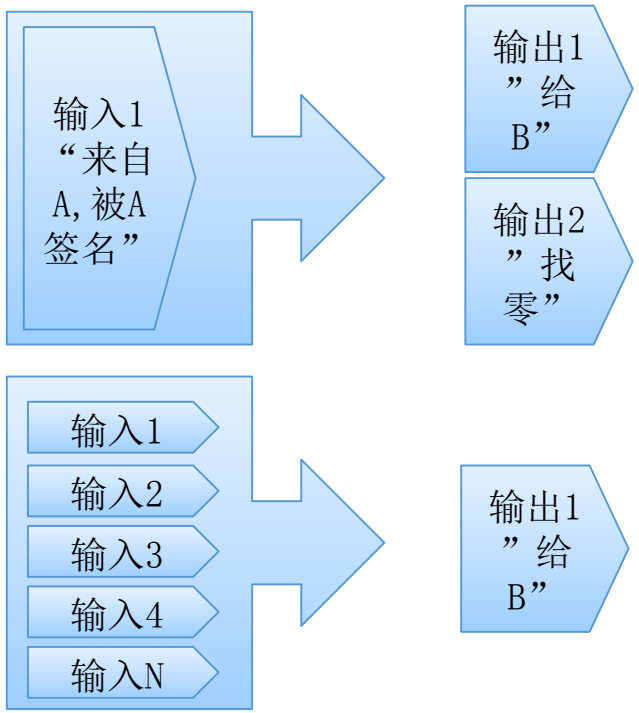
4. P2P数据传输，分布式网络存储



3. 共识机制（工作量证明PoW），防止链分叉

利用区块链技术避免支付中的“双花”



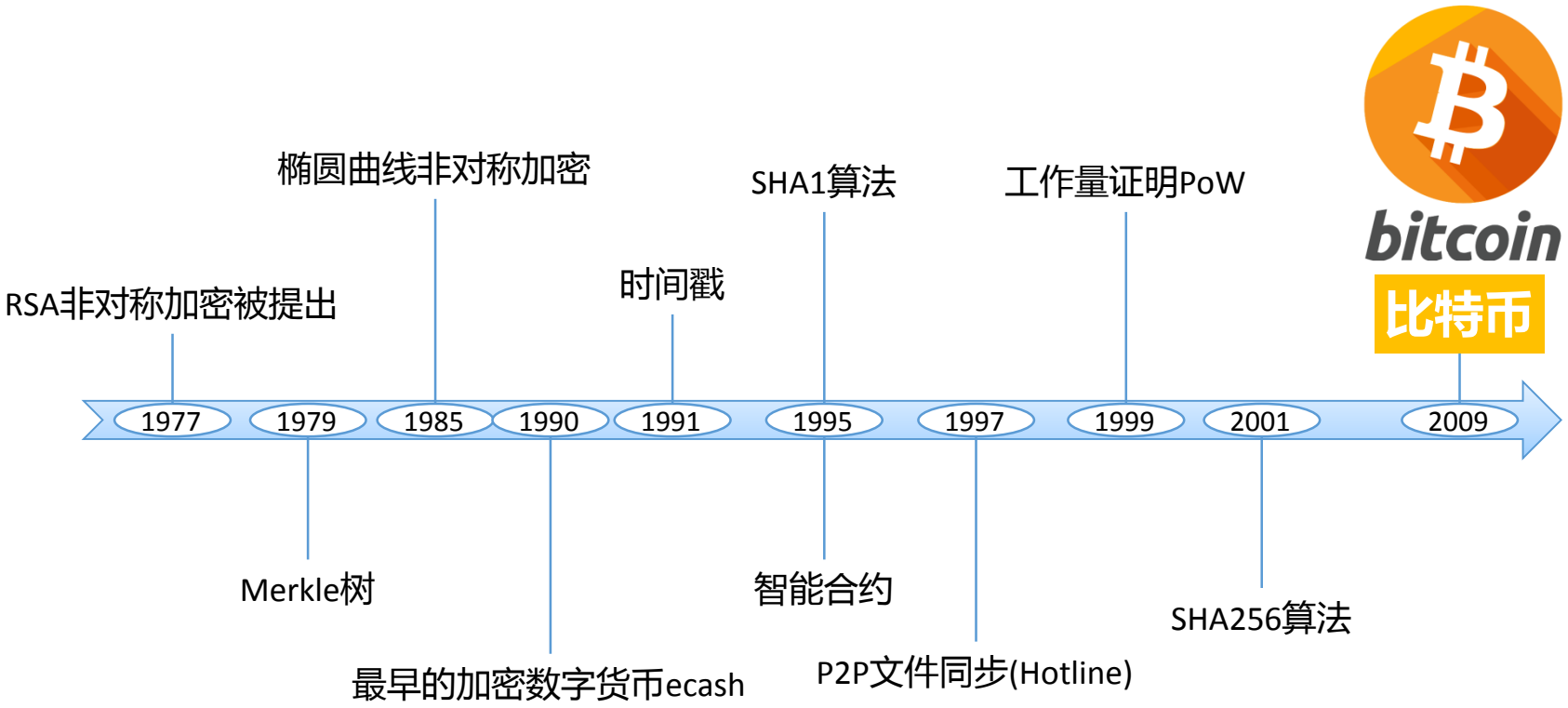


UTXO Unspent Transaction Output

数字签名和区块链数据结构确保交易不被篡改

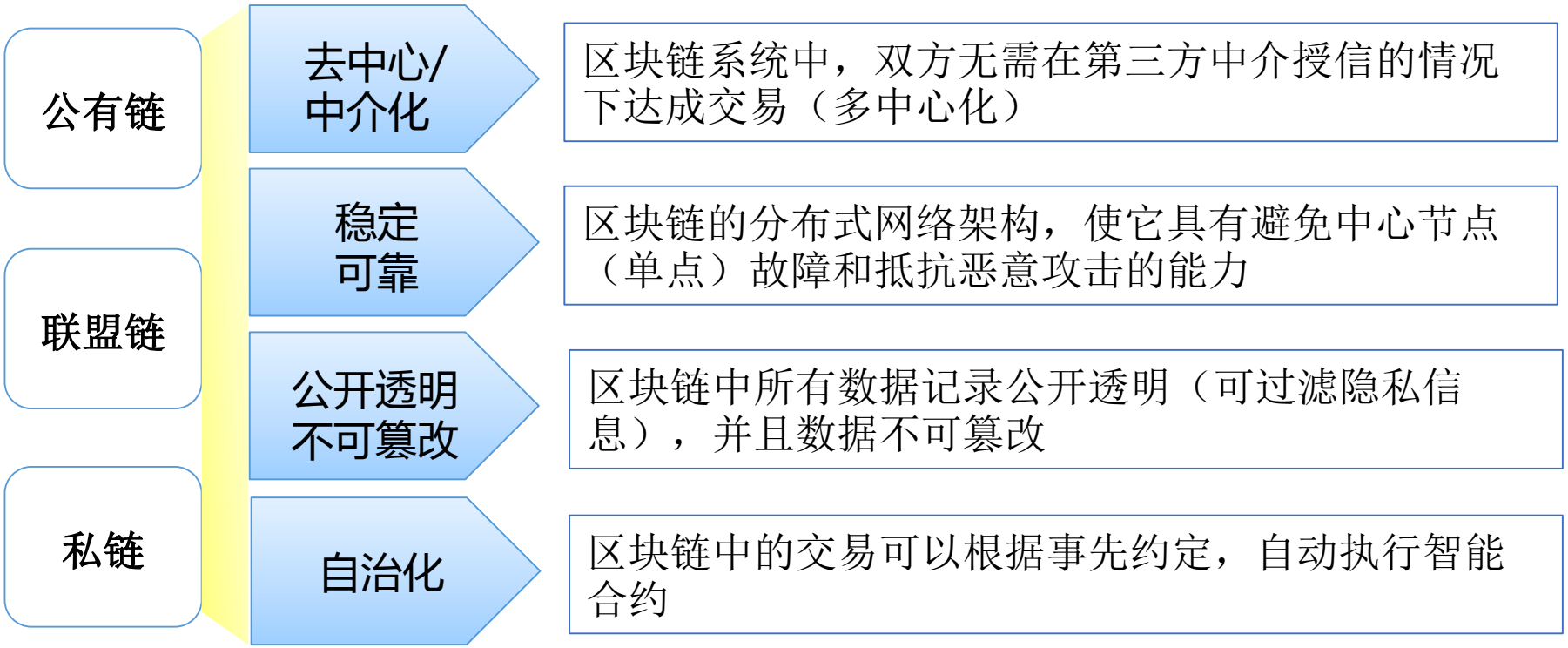
UTXO机制确保不会发生“双花”

成熟的技术也成产生颠覆式的创新



成熟的技术通过一系列巧妙的组合，最终创造了革命性的产品！

区块链技术的几个关键特点



大纲

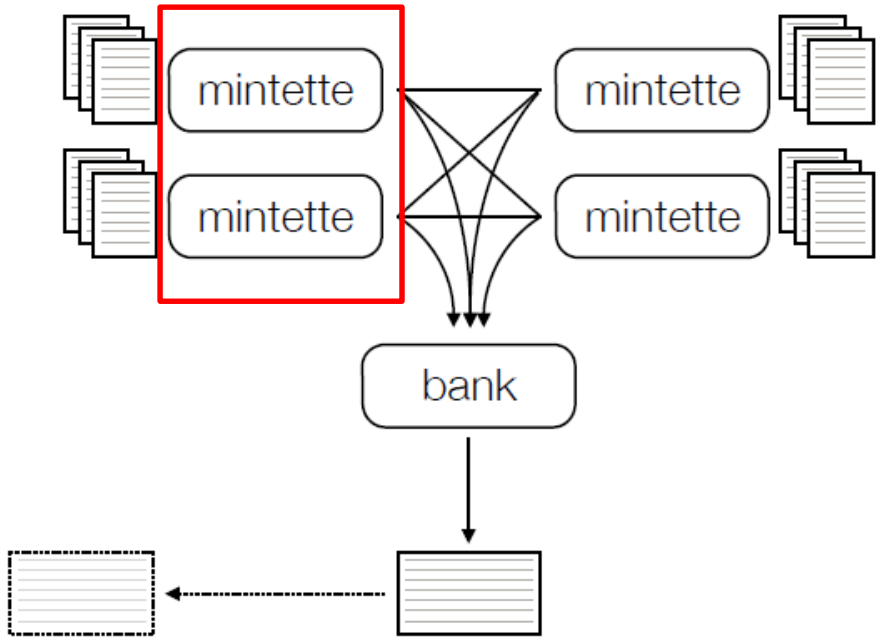
区块链的来源及特点

金融领域参考案例分析

互联网金融的区块链创新

英格兰银行RSCoin – 区块链构成

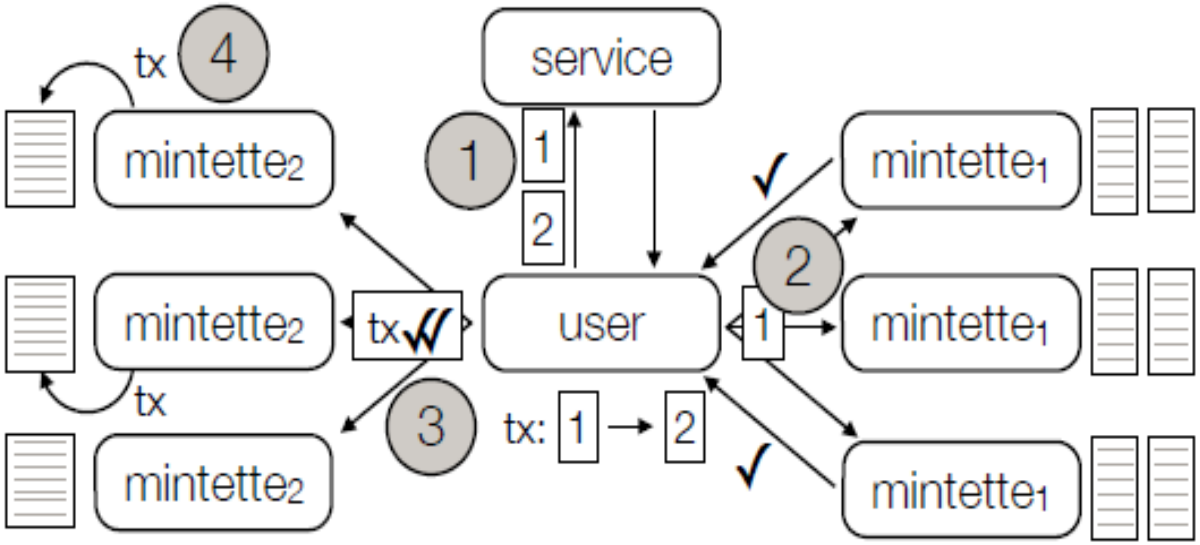
- RSCoin是由英格兰银行和伦敦大学合作开发的，由央行控制和发行的数字货币
- 实现机制
  - 分为两个角色：bank（中央银行）和mintette，bank向mintette签发包含公钥的证书
  - Mintette负责生成lower-level block，并上传给bank生成higher-level block



  - Mintette每隔一段时间(epcho 时长可变)生成一次lower-level block，mintette之间的block可能有交叉引用（提高交易吞吐量）
  - Mintette每隔较长时间(period)将lower-level block上传给bank，bank生成higher-level block，并构成主区块链

引自：Centrally Banked Cryptocurrencies

英格兰银行RSCoin – 防止双花机制



步骤：

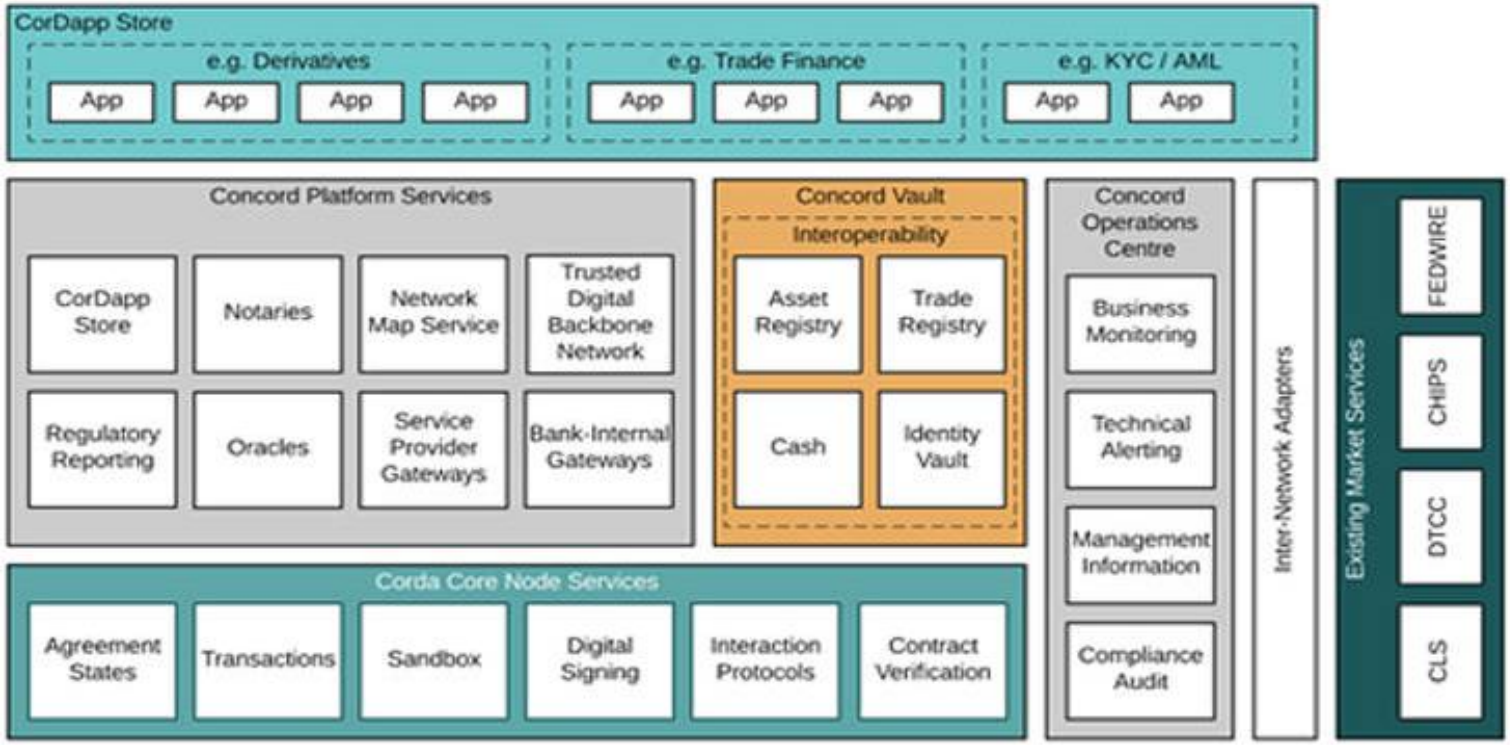
1. 查询addrid归属
2. 向对应的mintette确认input addrid没有被消费
3. 通知output addrid 的mintette确认交易
4. mintette记录交易到block

- 交易记录通过addrid随机分组，每组addrid分布到多个mintette中存储
- 在RSCoin中，addrid有类似UTXO的功能；每次交易采用2PC两阶段提交的方式完成，确保不会发生双花

引自：Centrally Banked Cryptocurrencies

R3 Concord平台 – 连接银行和企业

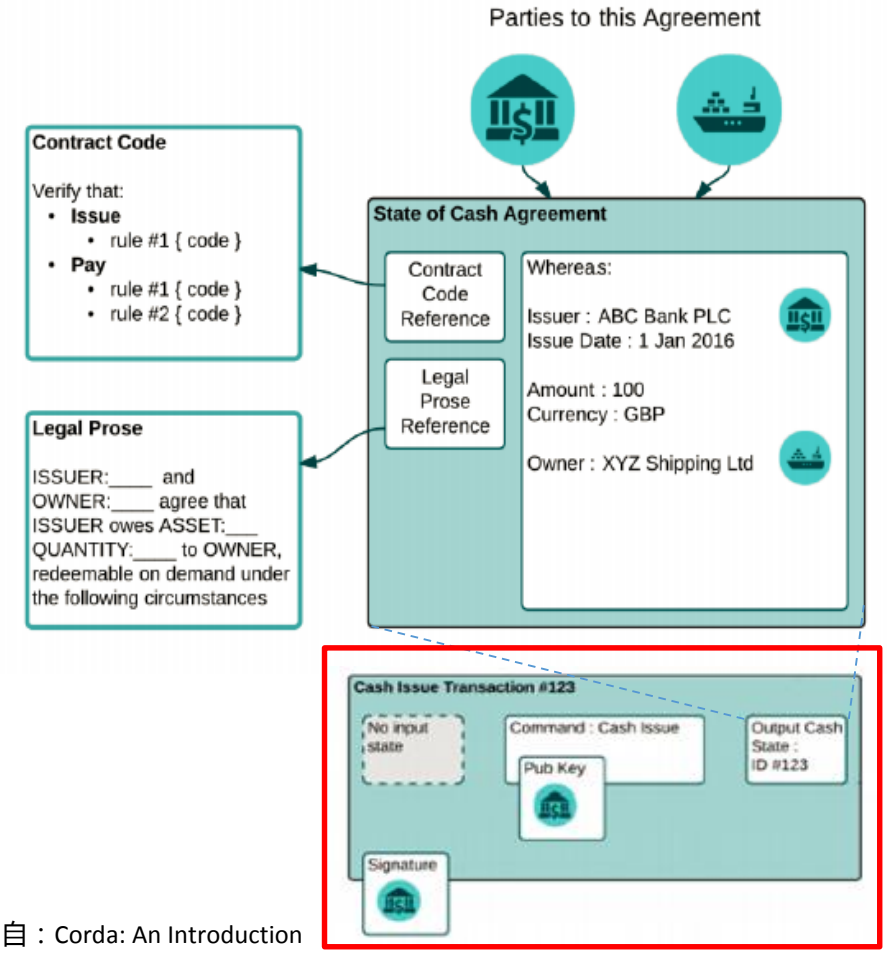
R3CEV（Crypto 2.0, Exchanges, Ventures) 是一家总部位于纽约的区块链创业公司，由其发起的R3区块链联盟，至今已吸引了42家巨头银行的参与，其中包括美国银行、汇丰银行等，中国已经有平安集团和招商银行等机构近期加入该联盟。



- Concord上层支持金融衍生产品、贸易融资等业务，中间层提供公共服务，其中Vault是Concord的区块链。Corda是Concord的底层基础平台。

引自：互联网上Concord介绍资料

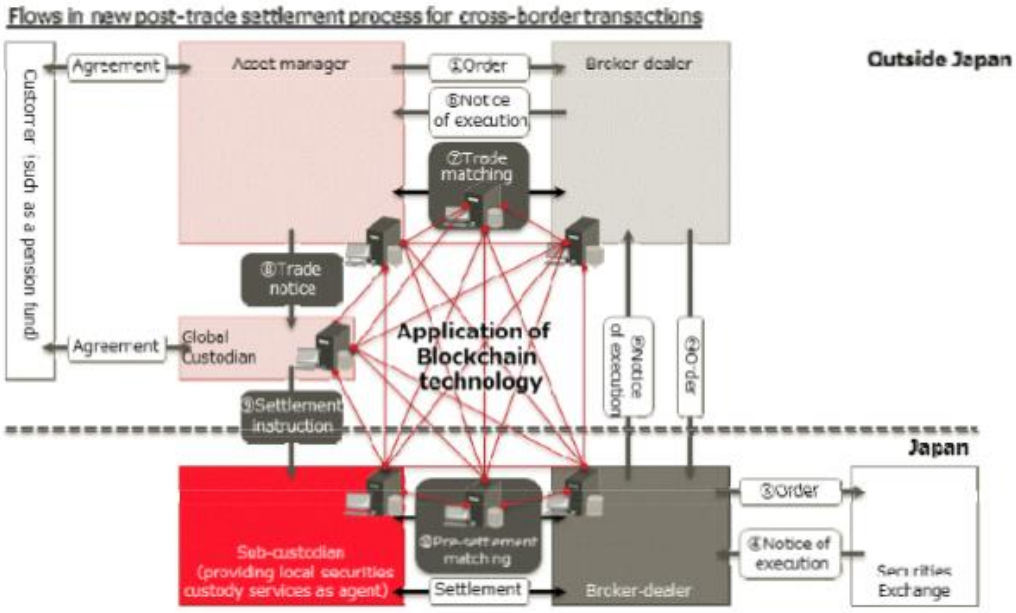
R3 – Corda 记录和处理金融智能合约的分布式账本



引自：Corda: An Introduction

- 设计思路
  - **数据一致性降低业务复杂性**
  - 账本信息的权威性
  - **不做全信息的全局共享**
  - 支持监管
  - **同时记录智能协议代码和合同文本**
  - 实现无中心模式的工作流
  - 采用类似UTXO机制来防止双花
- 关键概念
  - State Object: 协议及协议代码
  - Transaction: 转换State Object
  - Business Flow: 无中心工作流
- 例子：银行发行电子货币

日本瑞穗银行基于区块链的跨境证券交易系统



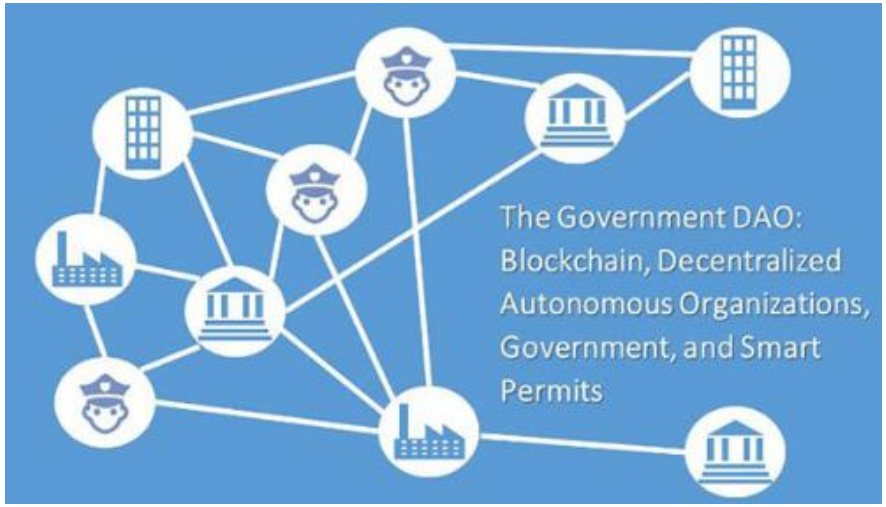
MIZUHO

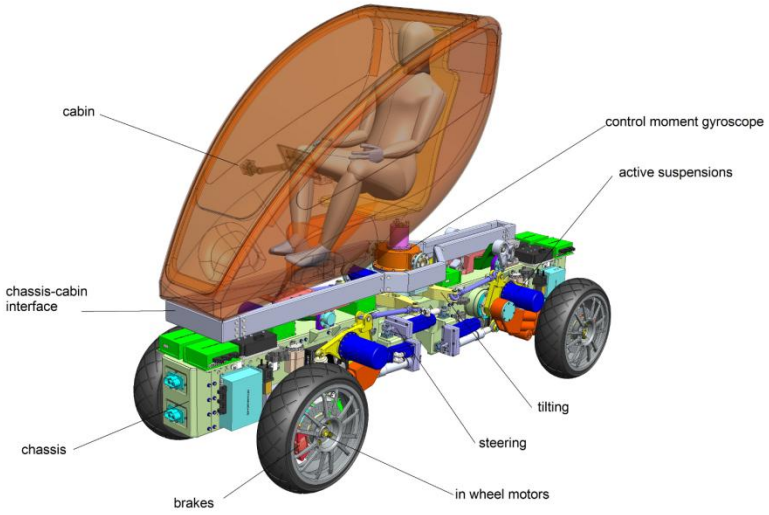
瑞穗实业银行

- 与富士公司合作开发基于区块链的跨境证券交易系统
- 通过简化业务处理，新系统的开发将缩短了交易处理时间，从**T+3**缩短至**T+0**
- 瑞穗银行**曾经尝试建立中心化的系统**解决操作复杂性问题，但是由于成本原因没有成功
- 于2016年3月份完成了试运行

图片引自：互联网上介绍资料

以太坊 The DAO 去中心化自治组织





- 以太坊(Ethereum)是一个开放的，去中心化的，图灵完备的区块链平台，可以构建去中心化应用(Dapp)和智能协议
- **The DAO全称是Decentralized Autonomous Organization，即“去中心化的自治组织”，可理解为完全由计算机代码控制运作的类似公司的实体**
- The DAO 是搭建在以太坊平台上，它运用以太坊的智能协议实现了众筹超过1.6亿美元， The DAO本质上是个VC（风险投资基金）
- 右上图是The DAO中Mobotiq项目的产品设计

引自：图片互联网上介绍资料及Mobotiq官网资料

国内区块链实践方兴未艾，联盟组织不断涌现

联盟名称	创立时间	描述
中国区块链研究联盟	2016年1月5日	全球共享金融100人论坛在北京宣布成立“中国区块链研究联盟”
中关村区块链产业联盟成立	2016年2月3日	全球首家专注网络空间基础设施创新的中关村区块链产业联盟在京成立
中国分布式总账基础协议联盟 ChinaLedger	2016年4月19日	中证机构间报价系统股份有限公司等11家机构共同发起
金融区块链合作联盟	2016年6月1日	微众银行、平安银行、京东金融等25家企业发起，腾讯和华为等6家机构作为成员单位加入
中国区块链技术和产业发展论坛	2016年10月18日	工信部和国标委指导下成立，副理事长单位包括蚂蚁金服等，海航生态科技是理事单位之一

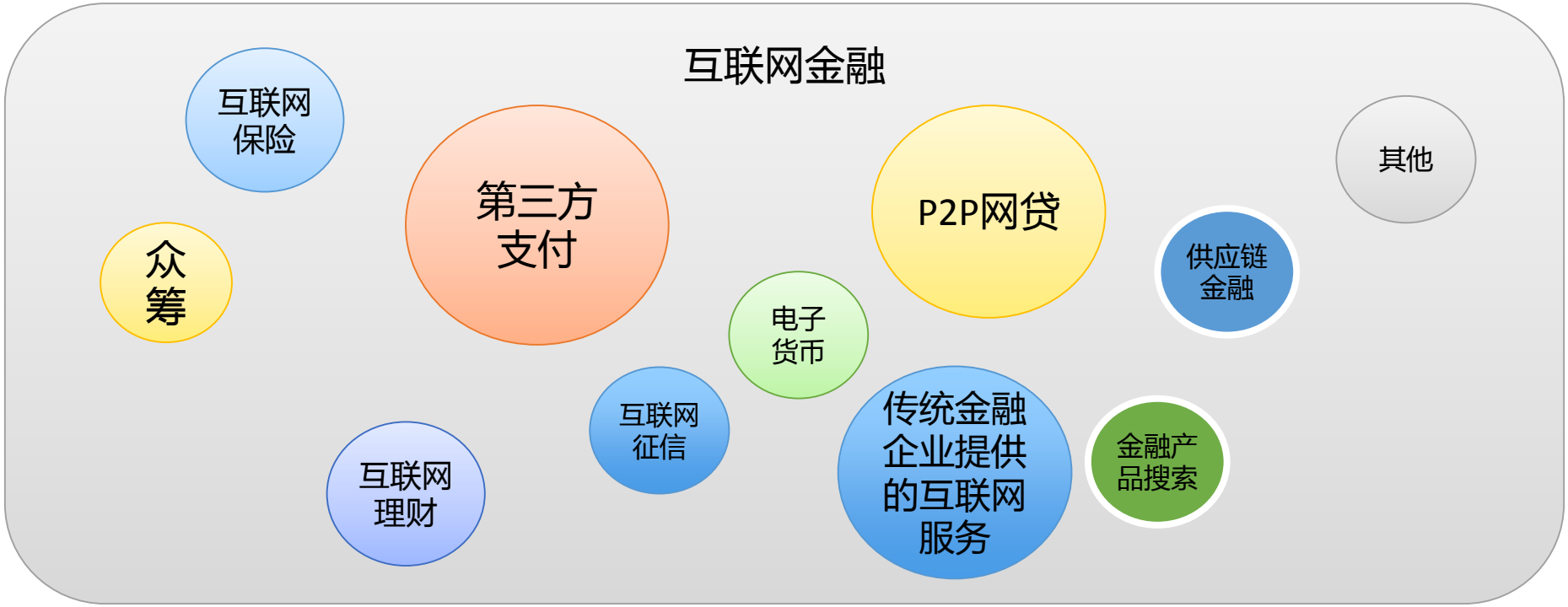
大纲

区块链的来源及特点

金融领域参考案例分析

互联网金融的区块链创新

当互联网金融遇到区块链

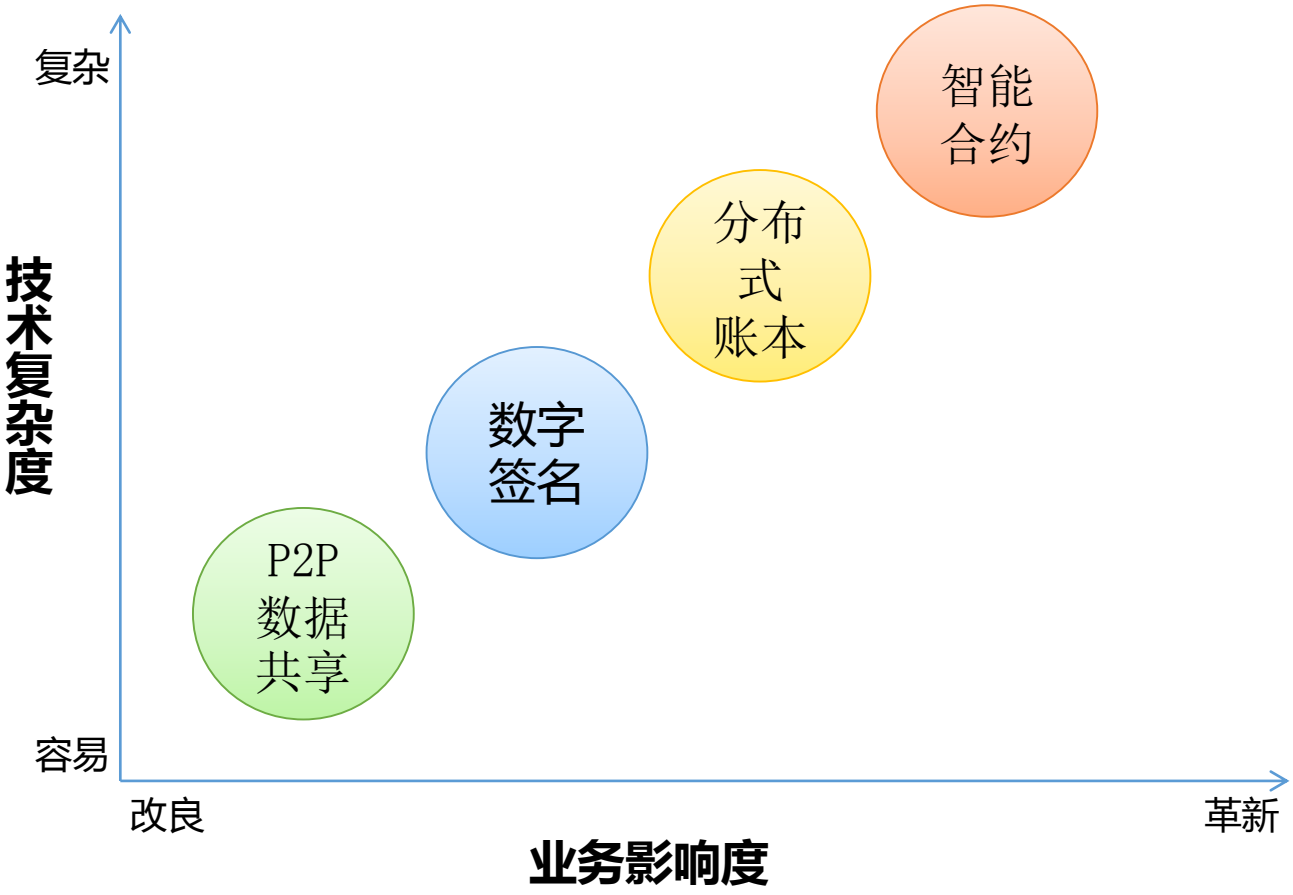


特点
- 中心化的信用
- 离散的数据
- 离散的业务逻辑

痛点
- 客户识别(KYC)成本高
- 业务背景真实性不好保证
- 清算结算等业务复杂

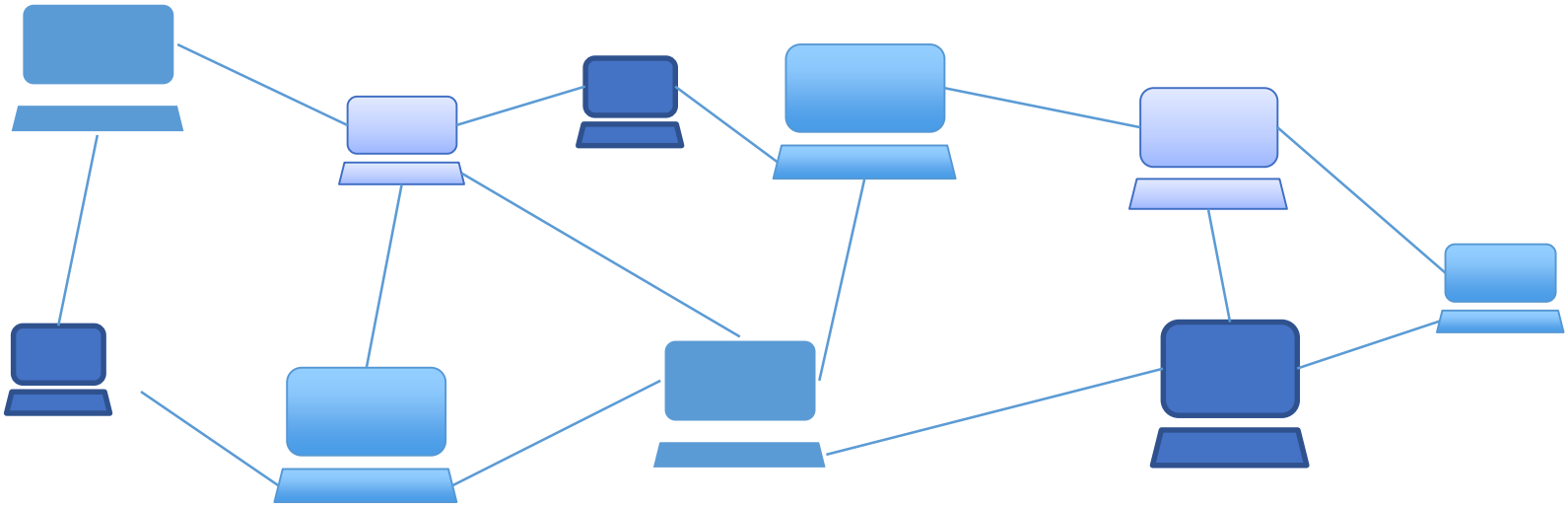
机会
- 客户识别与反洗钱
- 资产数字化
- 跨境支付及清结算
- ……

从渐进式优化开始，成熟的技术也能激发业务变革



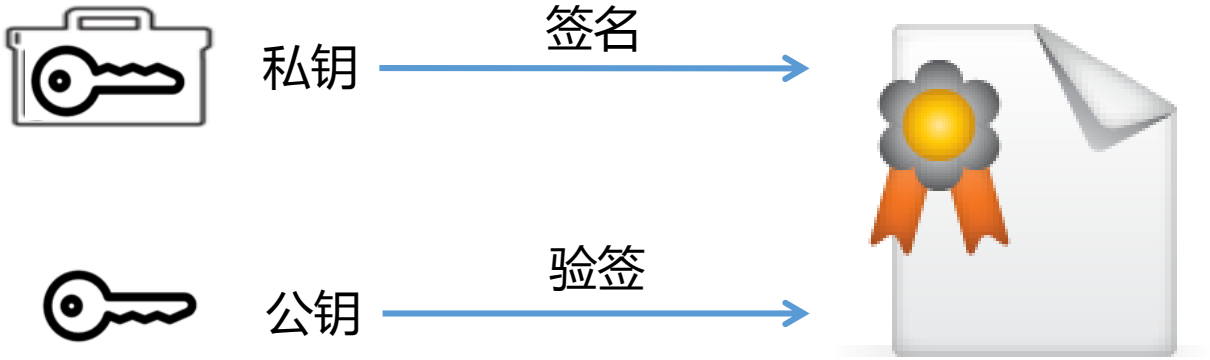
注：本图仅用于分析，并不代表区块链技术使用的路径

关键技术1 – P2P数据共享



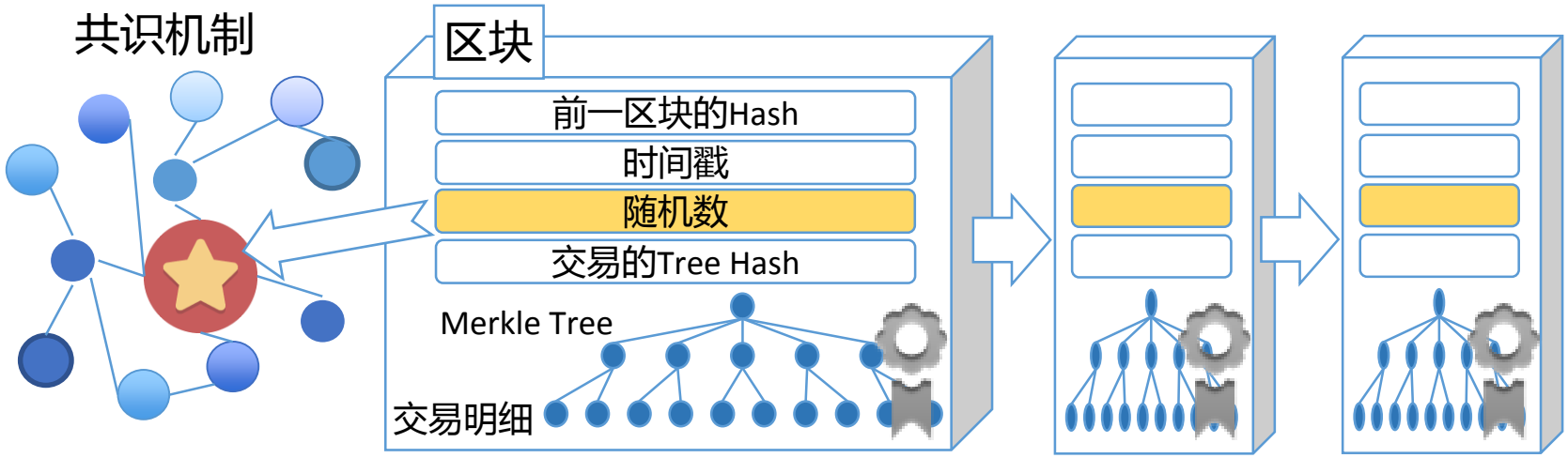
- **目前常用方法**
  - ✓ 中心化方式共享信息，例如RPC、 MQ、 FTP
  - ✓ 例如日终对账
- **区块链使用方法**
  - ✓ 实现点对点准实时数据分享
  - ✓ 去中心化网络，更健壮
- **启示**
  - ✓ P2P方式分享数据可以提高效率，优化业务处理

关键技术2 – 数字签名



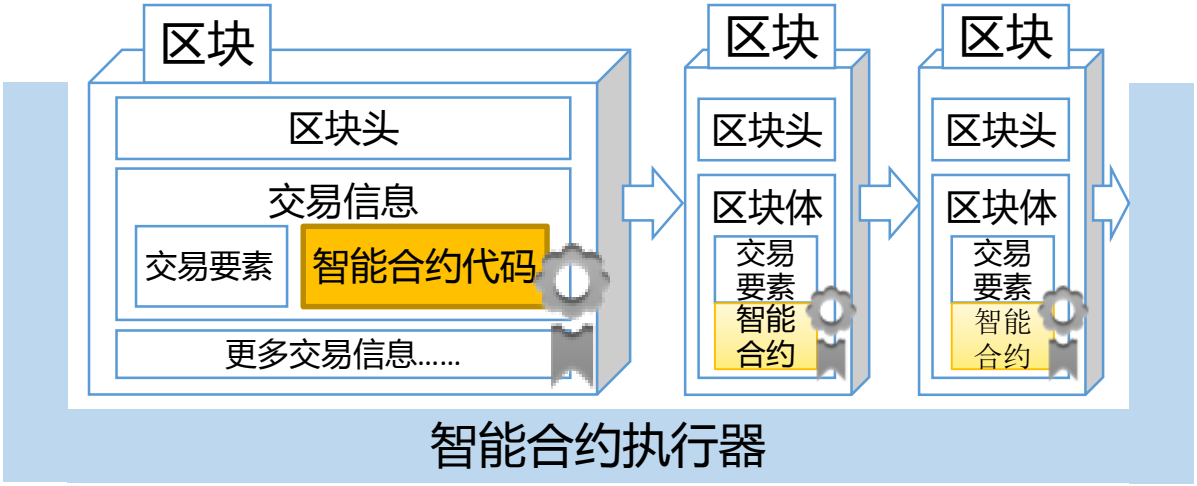
- **目前常用方法**
  - ✓ 签名更多只作为认证方法
  - ✓ 业务数据还要通过多种方式进行比对
- **启示**
  - ✓ 只检查签名可以降低处理复杂度
- **区块链使用方法**
  - ✓ 只信任数字签名
  - ✓ 不做更多数据核对

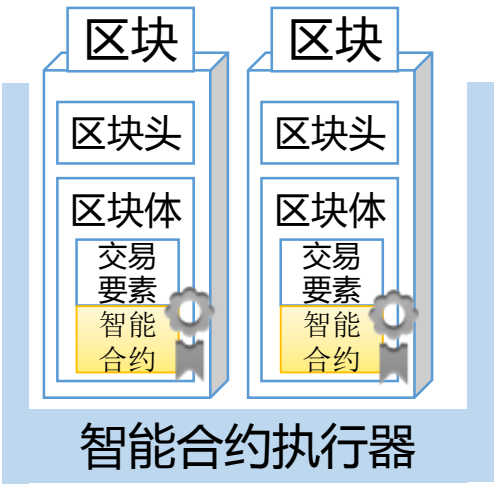
关键技术3 – 分布式账本



- **目前常用方法**
  - ✓ 各自拥有数据备份
  - ✓ 各自拥有一部分私有数据
  - ✓ 多个数据副本通过复杂业务流程保持一致
- **区块链使用方法**
  - ✓ 所有人都能验证交易合法性
  - ✓ 通过共识机制确认记账权
  - ✓ 数据透明分享
  - ✓ 数据不可篡改
- **启示**
  - ✓ 通过不可篡改的数据分享，提升业务效率，实现更复杂的业务目标

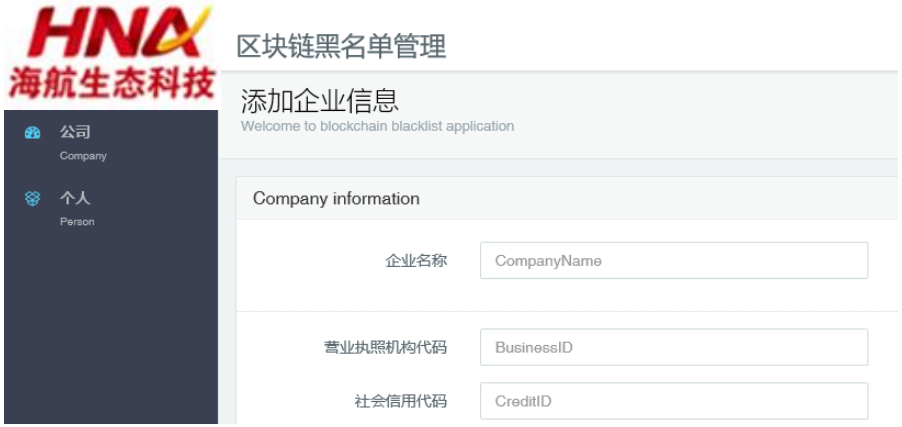
关键技术4 – 智能合约

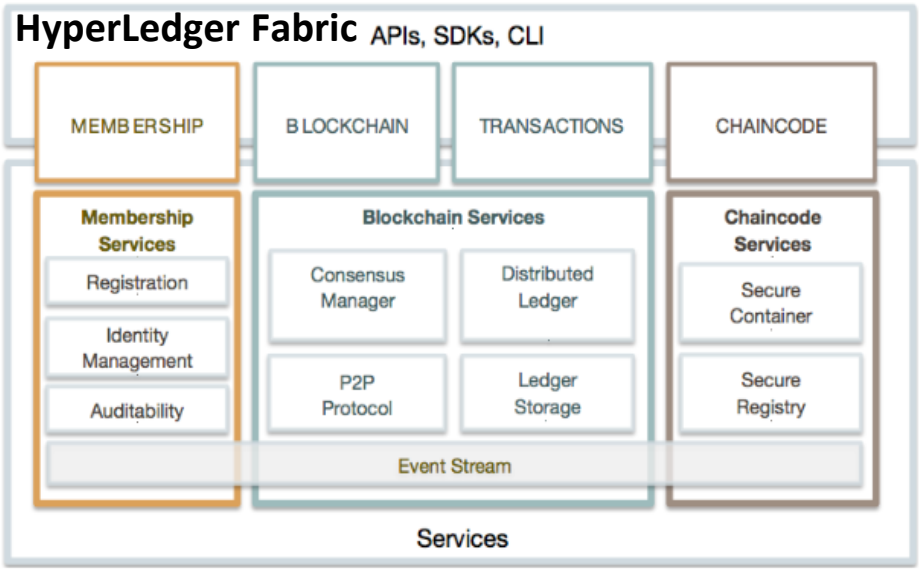




- **目前常用方法**
  - ✓ 业务逻辑在各个企业自己的应用中实现
  - ✓ 业务逻辑可能发生改变
- **区块链使用方法**
  - ✓ 将业务逻辑写到智能合约中，并签名记录到区块链进行
  - ✓ 一旦具备执行条件，自动执行智能合约
- **启示**
  - ✓ 去中心化方式的智能合约可以提升系统稳定性，增强信任

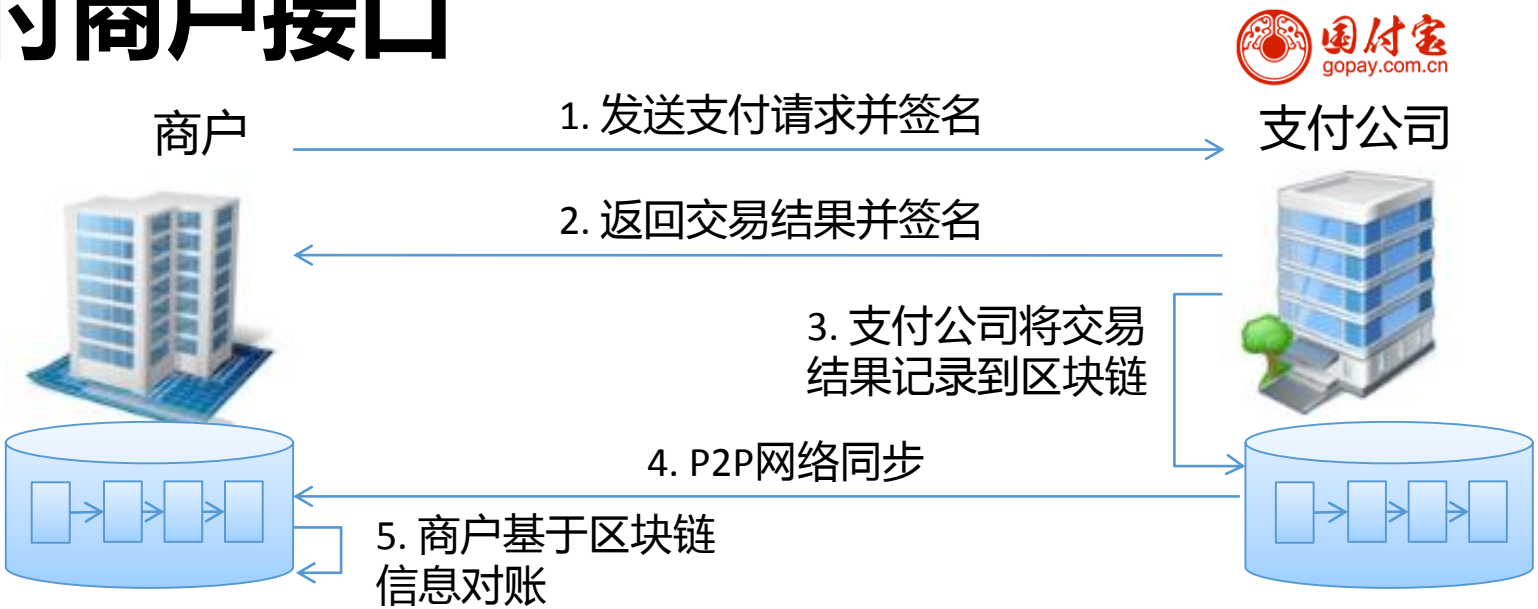
尝试1--海航生态科技区块链黑名单





- **需求来源**
  - 海航集团内部互联网金融企业众多，各自维护自己的黑名单信息
  - 国付宝、聚宝匯、海航通信等企业希望分享黑名单信息
- **利用到的区块链技术特点**
  - 区块链分布式账本+P2P数据分享，实现黑名单信息同步
  - 密钥加密签名，可追溯信息来源
  - 分布式部署，去中心化

尝试2—借鉴区块链技术优化第三方支付商户接口



- **需求来源**
  - 商户和支付公司之间的交易接口对信息一致性要求很高，以前的技术是通过单笔对账、批量对账的方式保证一致性
  - 利用区块链技术可以降低处理复杂度，提高效率
- **利用到的区块链技术特点**
  - 利用全局账本的权威性，尽快达成一致
  - 利用P2P网络同步，提高信息分享效率

金融领域新的区块链应用频频发布，但是总体技术和业务环境还有待完善

银联构建区块链电子凭证系统

微众银行运用区块链实现联合贷款

SWIFT推出区块链概念验证

中国央行数字货币研究所年底挂牌

回顾电子商务发展历程

90's

技术环境

- Unix
- J2EE
- WAS/Weblogic/.Net
- 互联网宽带尚未普及

业务环境

- 用户不信任网上购物

✓ 从操作系统到开发框架，开源工具的快速繁荣和成熟
✓ 互联网基础设施完善
✓ 用户行为的培养，配套支付/物流等设施的完善
✓ 企业思路的转变

10's

技术环境

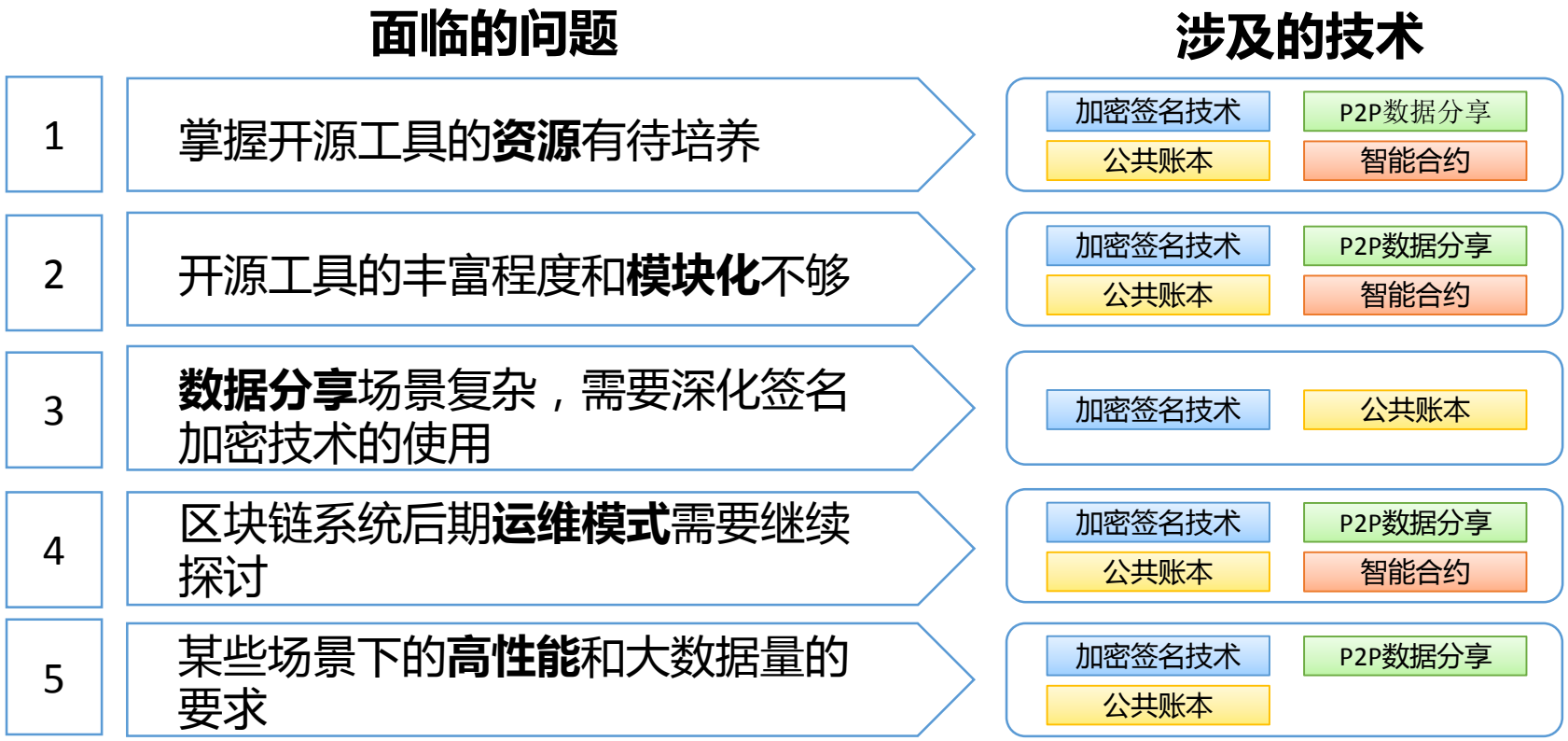
- Linux
- Tomcat/Spring等开源工具
- 互联网宽带已经普及

业务环境

- 接受了网上购物便利性

开源技术栈的完善，和企业内外部用户技术思想的转变，是区块链技术成熟的基础。

实践中遇到的典型问题


面临的问题
涉及的技术
1
掌握开源工具的**资源**有待培养
加密签名技术
P2P数据分享
公共账本
智能合约
2
开源工具的丰富程度和**模块化**不够
加密签名技术
P2P数据分享
公共账本
智能合约
3
数据分享场景复杂，需要深化签名加密技术的使用
加密签名技术
公共账本
4
区块链系统后期**运维模式**需要继续探讨
加密签名技术
P2P数据分享
公共账本
智能合约
5
某些场景下的**高性能**和大数据量的要求
加密签名技术
P2P数据分享
公共账本

未来区块链技术大规模运用时可能面临的问题

信息传递
基于TCP/IP的互联网

价值传递
基于区块链的信用体系

面临的挑战	主要涉及的区块链	建议的应对措施
互操作性	公有链 联盟链	制定区块链技术规范
数据一致性	公有链	完善互联网基础设施建设
行业监管	公有链 联盟链	制定行业规范 引导相关行业标准的制定

总结

一个系统越大、层次越多、越是**去中心化**，那么它在有机成长方面取得的进展也就越多。

----引自《失控》 凯文.凯利

提高效率，节省成本，业务创新

THANKS

ArchSummit
全 球 架 构 师 峰 会 2016

[北京站]

主办方 Geekbang. 极客邦科技 InfoQ