

# 区块链项目业务分析方法

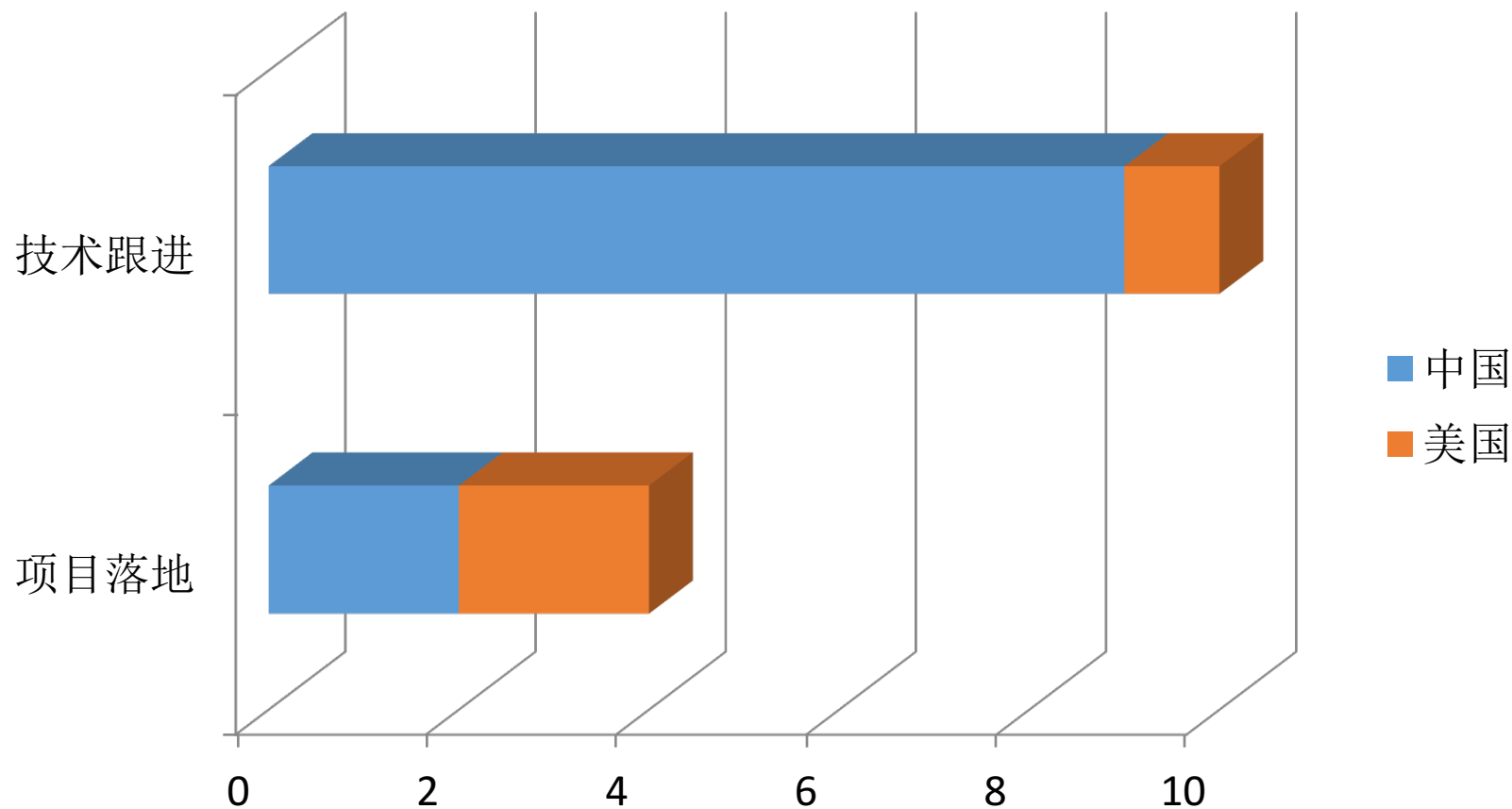
张蕾

2017年5月19日

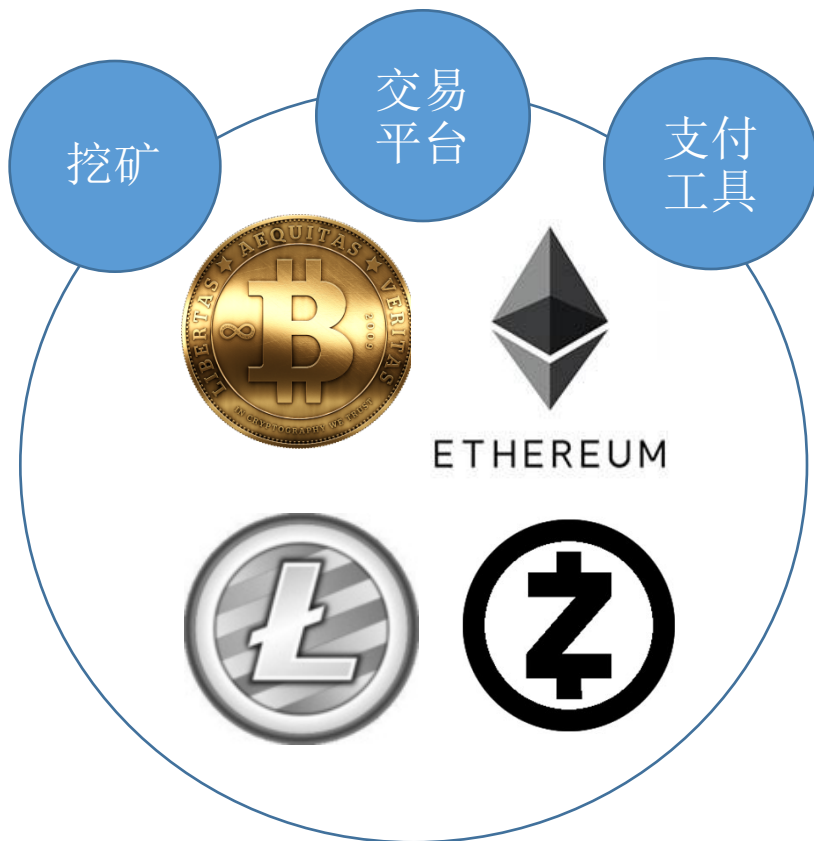
## 写在最前面的话

“Blockchain-enabled technology is changing the way companies approach commerce、trading、transparency、security、identification、supply chain、auditing and so much more—the most significant and valuable business systems in the world will be powered by blockchains.”

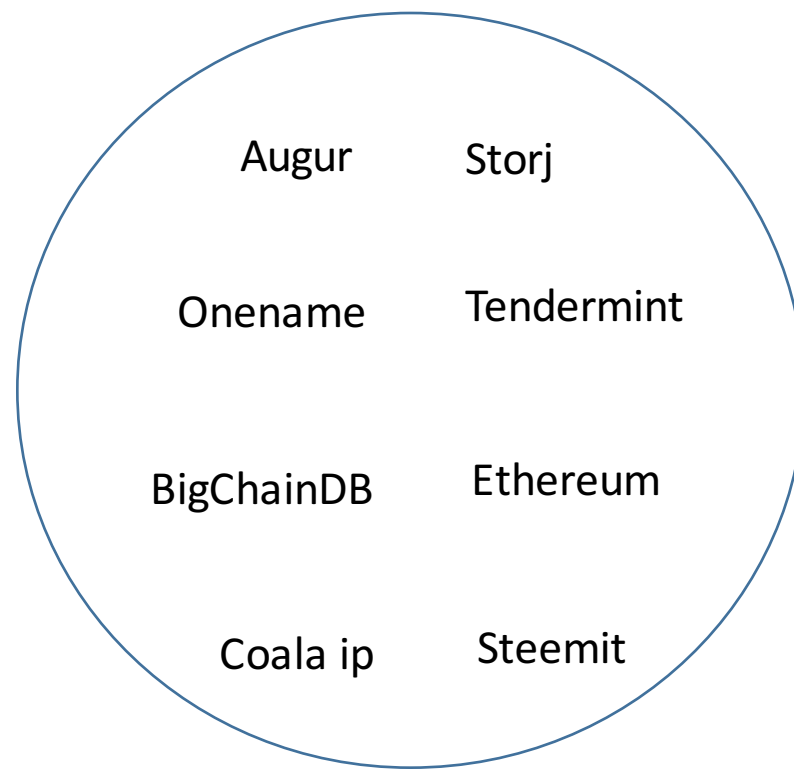
## 项目落地的速度远远落后于技术的跟进速度



# 世界上，区块链的“消费级”产品仍然是比特币



基本成熟



刚刚起步

# 在国内，技术与项目之间的鸿沟

## 真实的区块链需求

- 1、《人民的名义》电视剧提前剧透，如何用区块链防止剧透或者快速跟踪定位泄露的源头？
- 2、新农合骗保问题严重，区块链如何有效地解决这个问题？
- 3、我有3000万大学生的学历信息，如何区块链构建一个应用系统 SAAS，并且从中获利？

## 区块链创业项目

### 原生项目

防伪溯源

数字资产交易

存证

### 区块链原生功能

统一账本  
(内容不能修改)

共识机制

原生交易

加密哈希

### 主体

唯链

法链

小蚁

onchain

inchain

## “区块链业务分析”的概念

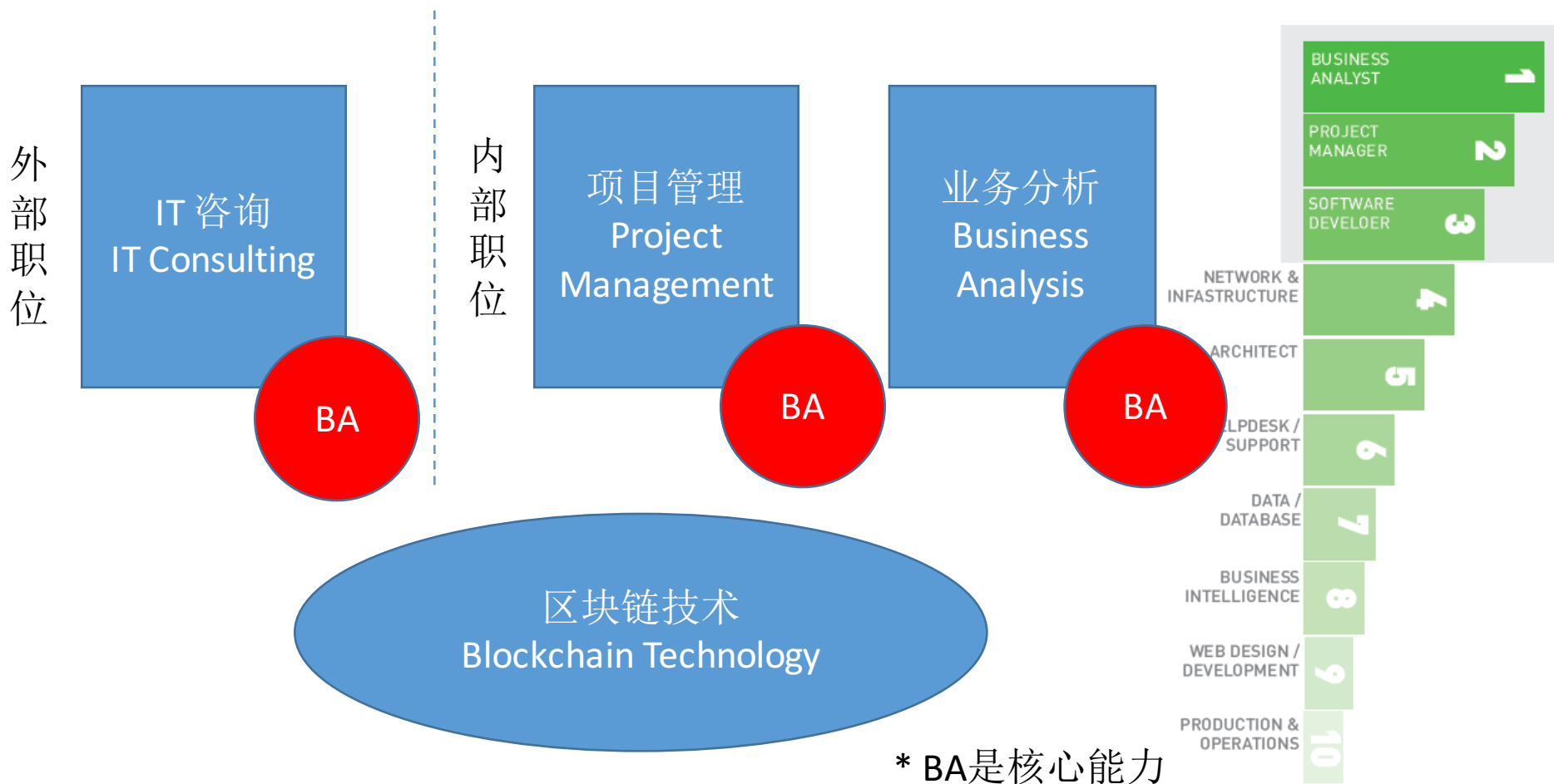


Business analysis is the set of tasks and techniques used to work as a liaison among stakeholders in order to understand the structure, policies, and operations of an organization, and recommend solutions that enable the organization to achieve its goals.

## 区块链业务分析

- Blockchain Business Analysis
- 基于IIBA的BABOK 3.0 标准

# 区块链人才的职业发展：Business Analysis都是核心能力



我们来开创一个新的职业

区块链业务分析师  
Blockchain Business Analyst

区块链需求分析师  
Blockchain Requirements Analyst



## 区块链业务分析的核心点概述



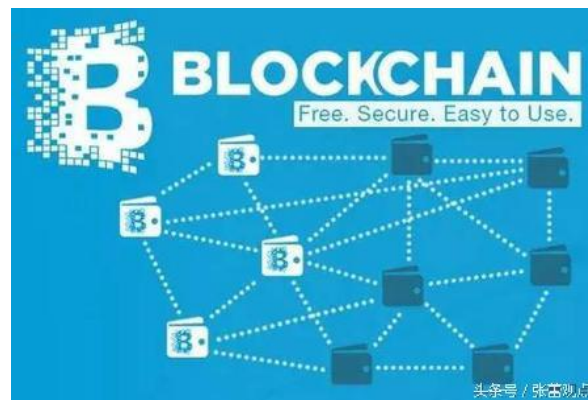
一个中心、六个规则

## 分析的过程与“数据库系统”对比



数据库系统：

- 1、中心化数据存储
- 2、中心化的业务逻辑



区块链系统：

- 1、分布式的同步数据存储
- 2、去中心化的业务逻辑

第一原则：

凡是用数据库系统可以提供成熟的解决方案，用区块链就是很愚蠢的。

## 区块链业务分析标准解释：（1）



设计目标：去中心

设计重点：

- 1) 业务场景中，哪些功能需要去中心？
- 2) 为什么要去中心？
- 3) 去中心后，效率和安全性怎么保证？

## 区块链业务分析标准解释：（2）

设计目标：分布式网络



设计重点：

- 1) BS或CS架构；
- 2) 服务器和终端的分离；
- 3) 主机性能、集群；
- 4) 网络性能、CDN等。

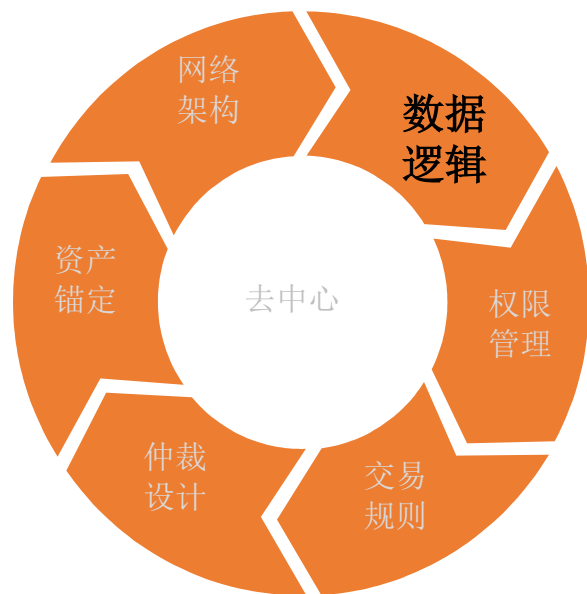


设计重点：

- 1) 分布式架构；
- 2) 服务器和终端合为一体；
- 3) 区块链内涵与区块链外延；
- 4) 完全节点和SPV节点；
- 5) 全球节点布局的地理位置和延迟速度；
- 6) 能源的消耗。

## 区块链业务分析标准解释：（3）

设计目标：数据与逻辑的分离



设计重点：

- 1) 数据层面的“存储过程”；
- 2) 业务逻辑更多集中在代码层面。



设计重点：

- 1) 逻辑和数据耦合紧密；
- 2) 链上逻辑（智能合约）与业务逻辑的分离；
- 3) 区块链与外部数据源的交互。

## 区块链业务分析标准解释：（4）



设计目标：权限与授权

设计重点：

- 1) 权限是如何划分的？
- 2) 在去中心化的系统中，谁有权力给其他人设定权限？



## 区块链业务分析标准解释：（5）



设计目标：规则的制定

设计重点：

- 1) 区块链系统中哪些交易是合法的、被接受的，哪些是被拒绝的？
- 2) 不同操作者发起的交易之间存在互相依赖的关系是什么？



比如A向B发起一个交易，B又向C发起一个交易，这种情况B的交易就依赖于A的交易。如果不验证A交易的合法性，也就无法验证B交易的合法性。这种关于交易规则的设计，与传统的数据库中的规则相比要更复杂。



## 区块链业务分析标准解释：（6）



设计目标：仲裁者的选择

设计重点：

- 1) 仲裁是保证区块链分布式系统稳定运营的核心，仲裁者的首要任务就是消除分歧。
- 2) 明确哪些节点（或用户）充当仲裁者的角色？它们仲裁的内容和标准是什么？



仲裁者跟中介是有本质区别的，仲裁者对数据操作的权限要小得多，他们不能虚假交易或者违反规则修改数据内容。在金融系统案例中，仲裁者不能花别人的钱，也不能改变资产的总数量。

## 区块链业务分析标准解释：（7）

设计目标：区块链数据与实际资产的对应关系



设计重点：

1) 谁拥有这个系统，谁能控制数据库，谁就对资产锚定负责。



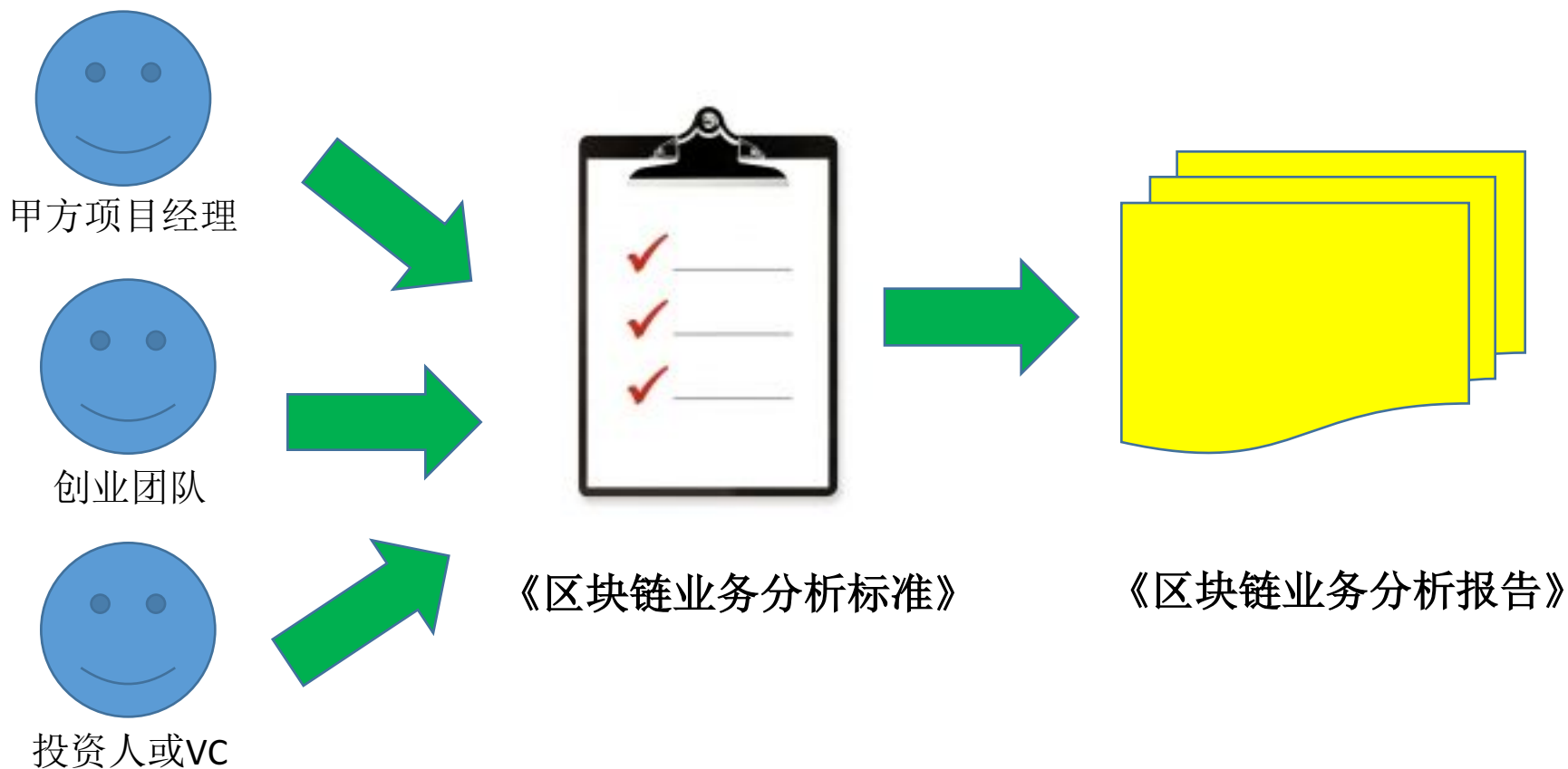
设计重点：

1) 在区块链系统中，可能存在多个法律主体、多种资产，甚至所有人对数据都有修改的能力。

2) 谁来为区块链中的交易数据做背书？

我在区块链上有十个单位的资产，谁能给我兑换现实世界的十个单位资产？或者说，如果没人给我兑换，我找谁去起诉或索赔？

## 区块链业务分析标准的应用



# 区块链业务分析案例

Blockchain Business Analysis Case

问题：

从业务分析的角度，

区块链在哪些领域更容易成功？

## 区块链的两个“致命”的问题

### 去中心化

技术语言描述就是，区块链允许系统中多个参与者，在并不信任对方的基础上，直接地、安全地共享一个数据信息，而不需要第三方中介的担保。这和很多传统的业务运作模式和监管体制是不相符合的。

### 丧失保密性

区块链系统中所有参与者，都可以查看到所有的交易记录，即使采取加密算法，区块链也会比传统数据库系统，泄漏更多的交易信息。而保密性是应用系统对客户的最基本的承诺。

总结来说：

**区块链代表了一种新的交易方式，  
它通过放弃部分的保密权利，  
来换取去中心化的权利。**

最适合区块链的应用特征是：

**轻量级的、多对手直接交易系统**



## 1) 什么是轻量级？

是指系统中，利益相关人比较少或者交易参与者的数量比较少。

在这种情况下，对保密性的要求不是特别突出。

## 2) 什么是多对手直接交易？

指交易的决策是多个对手直接作出的，可以使用或者不使用中介，中介对交易的本质不产生作用，只是在效率上有影响。

相对而言，去掉中介后，交易的效率 and 安全性更高。

## 典型的区块链应用

众筹	招投标	拍卖
博彩 (彩票)	商业积分	.....

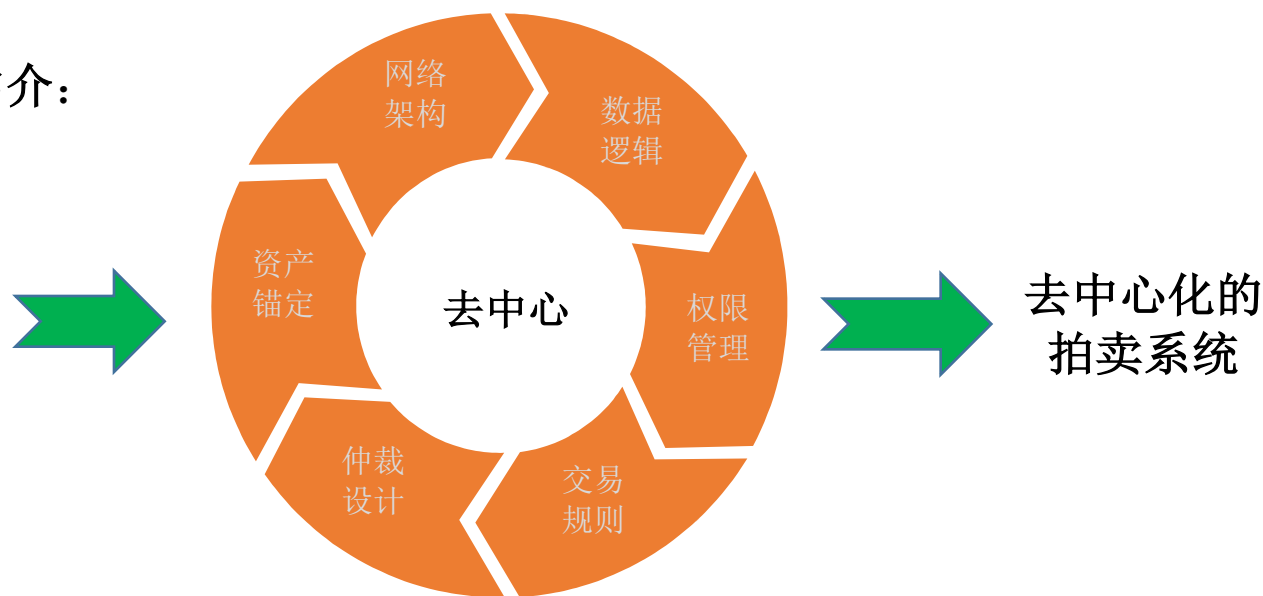
# 案例一 区块链拍卖系统

# 如何把中心化的拍卖系统改造成去中心化的系统？

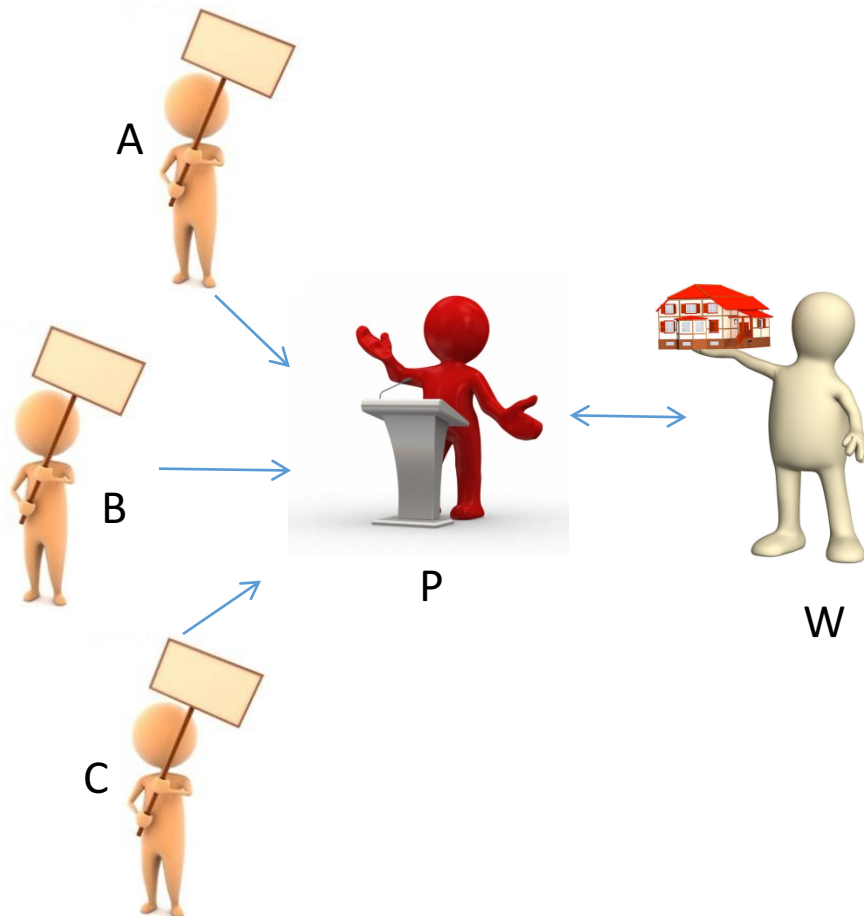
传统的拍卖公司作为中介：

- 1) 推广与宣传；
- 2) 活动的组织；
- 3) 双方的交易担保；
- 4) 参与到交易过程。

风险在这里产生！



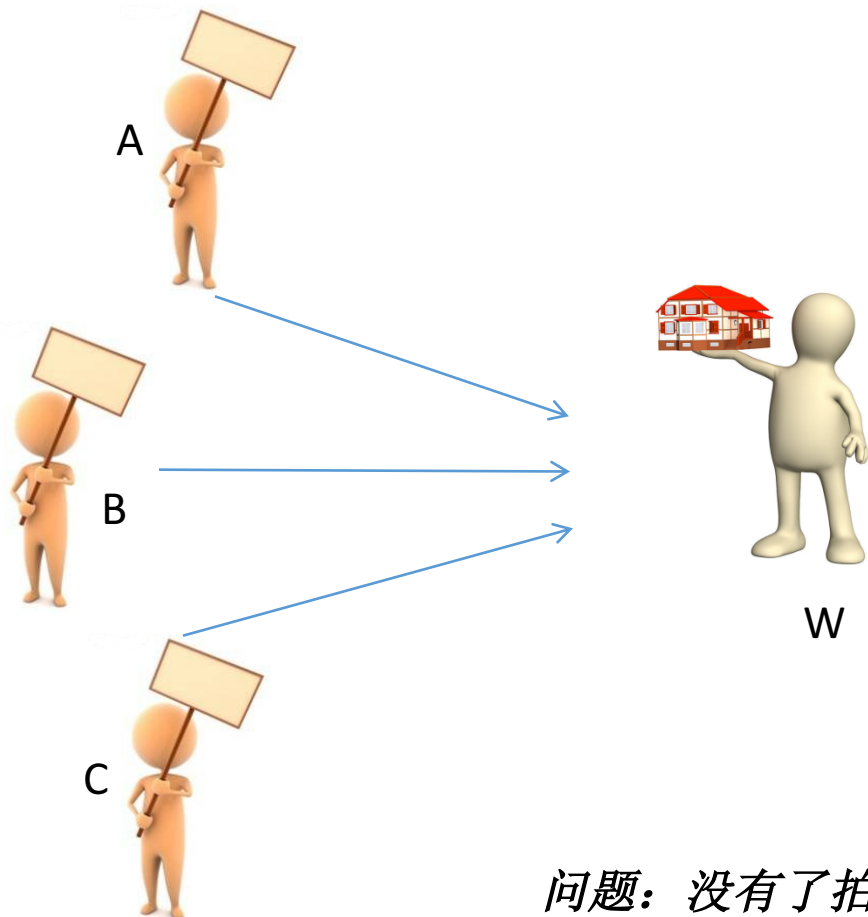
## 传统由拍卖公司主导的过程



涉及的主要交易过程：

- 1、ABC向P缴纳保证金；
- 2、ABC向P公开报价；
- 3、中标者通过P与W完成交易；
- 4、P向未中标者退还保证金。

## 去中心化的直接交易过程



涉及的交易过程：

- 1、ABC向W缴纳保证金；
- 2、ABC向W公开报价；
- 3、中标者与W完成交易；
- 4、W向未中标者退还保证金。

问题：没有了拍卖公司，直接交易的安全性怎么保证？

# 基于区块链来实现这个去中心化的交易过程

Input: x; Pay 55 to W, 45 to A

SIGNED(A) SIGNED(W)

...

Input: y; Pay 100 to A, LOCK until time  $t$

SIGNED(A) SIGNED(W)

Input: x; Pay 10 to W, 90 to A

SIGNED(A)\_\_\_\_\_

Input: x; Pay 05 to W, 95 to A

SIGNED(A)\_\_\_\_\_

Input: x; Pay 01 to W, 99 to A

SIGNED(A)\_\_\_\_\_

Input: y; Pay 100 to A/W (MULTISIG)

SIGNED(A)

拍卖成功!

咱们完成拍卖交易，我发布到区块链上!



A



W

## 案例二 区块链积分系统



积分是国际上普遍使用的、经过成功验证的一种商业营销工具...

1) 用积分来发起促销活动，适合长期营销，效果持久，成本低廉；

2) 用积分来维护客户关系，刺激多次消费，增强客户忠诚。

### 世界著名积分品牌

英国	Nectar
美国	Upromise
澳大利亚	fly buys
日本	TP卡
韩国	OkCashBag
台湾	happy go

积分价值在于流动性。通用积分（或积分联盟）是积分发展的必然趋势...

### 企业独立积分

积分（发行量、发行价格、兑换规则）完全被企业控制；

积分流动性差；

积分超发，积分贬值；

消费者参与热情低。

12%

### 通用积分或积分联盟

多种积分可以通存通兑；

兑换渠道广；

品牌价值相互提升；

积分兑换率高。

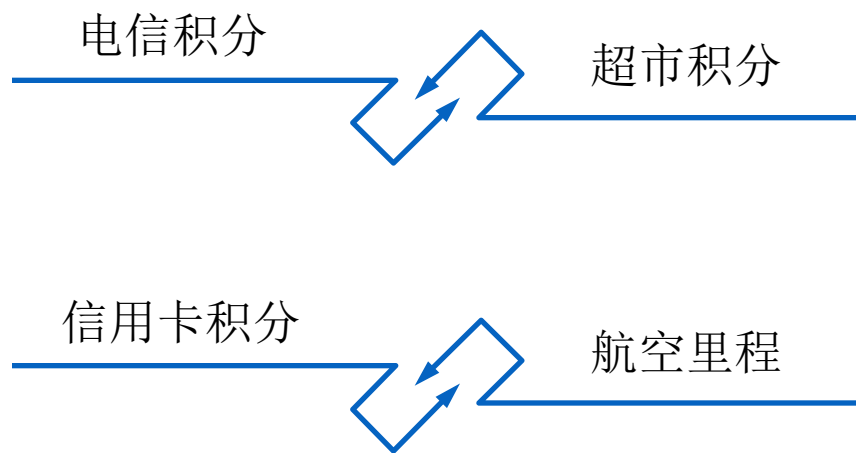
50%

积分兑换率

最佳实践

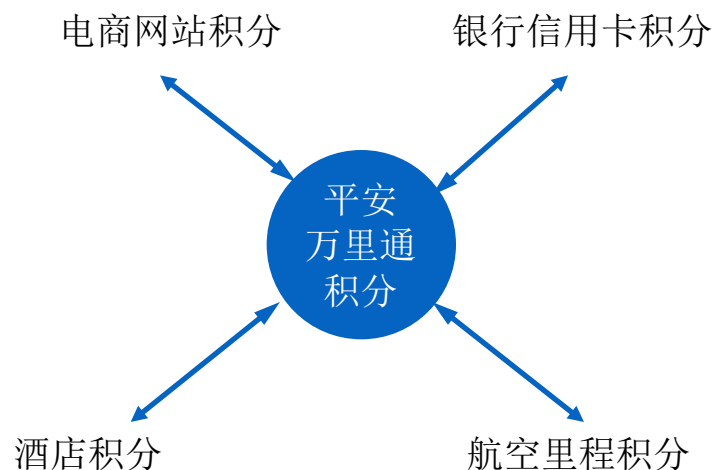
## 传统的模式，做通用积分离不开“中介”

方式一：积分互换



组织型中介

方式二：中介型积分

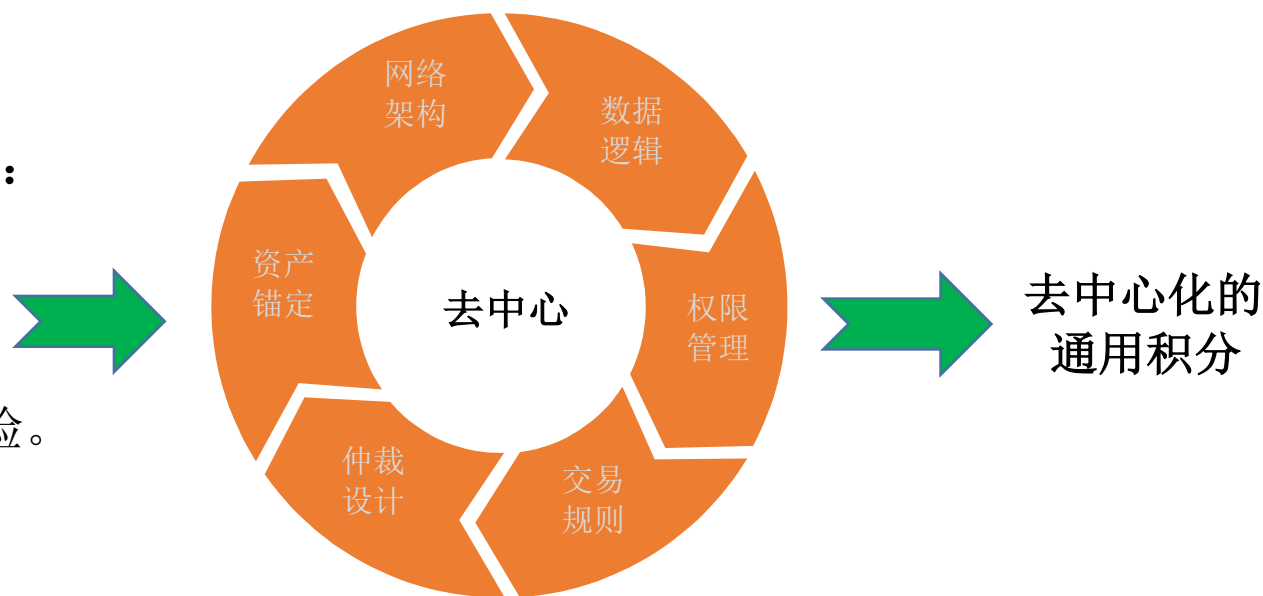


产品型中介

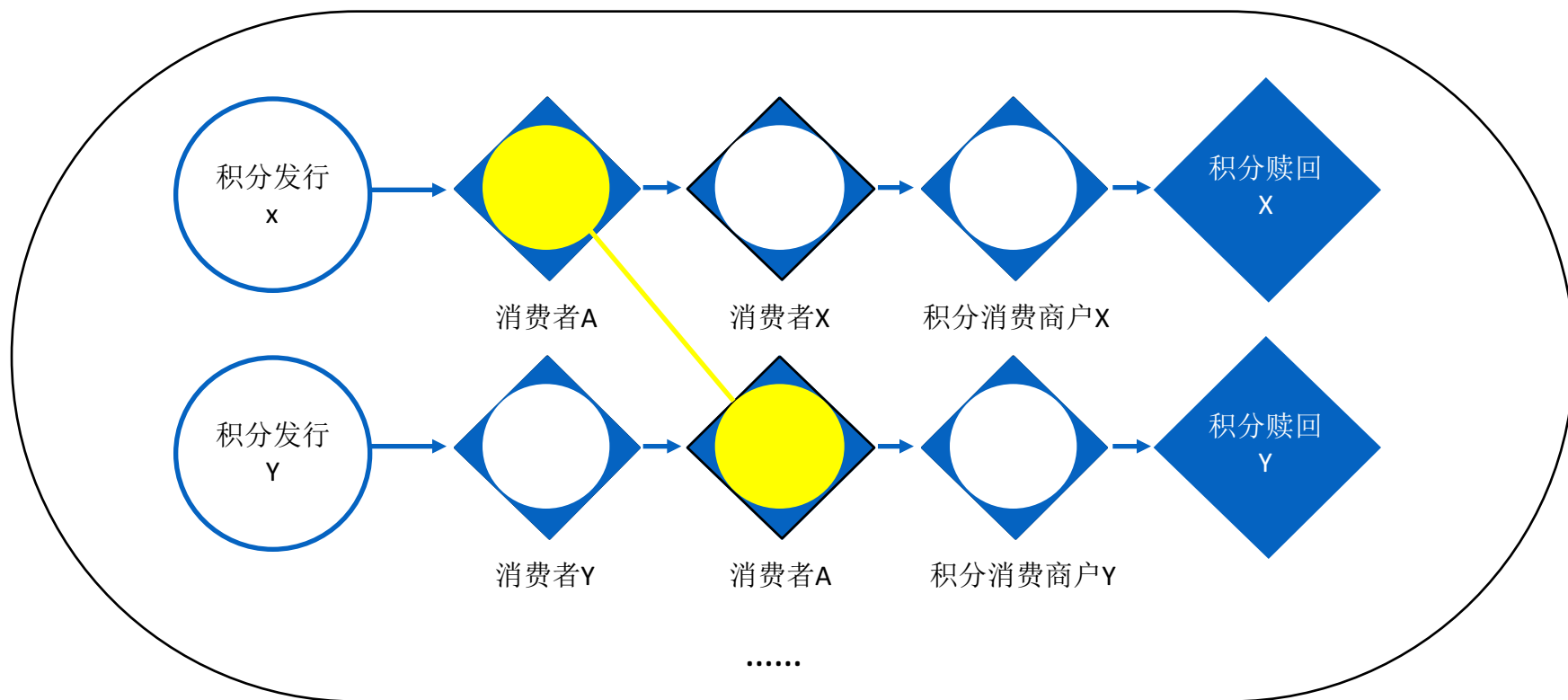
## 如何把中介型的通用积分改造成去中心化的通用积分？

中介型通用积分的风险：

- 1) 流通范围的受限；
- 2) 兑换费用的损失；
- 3) 中介本身的信用风险。

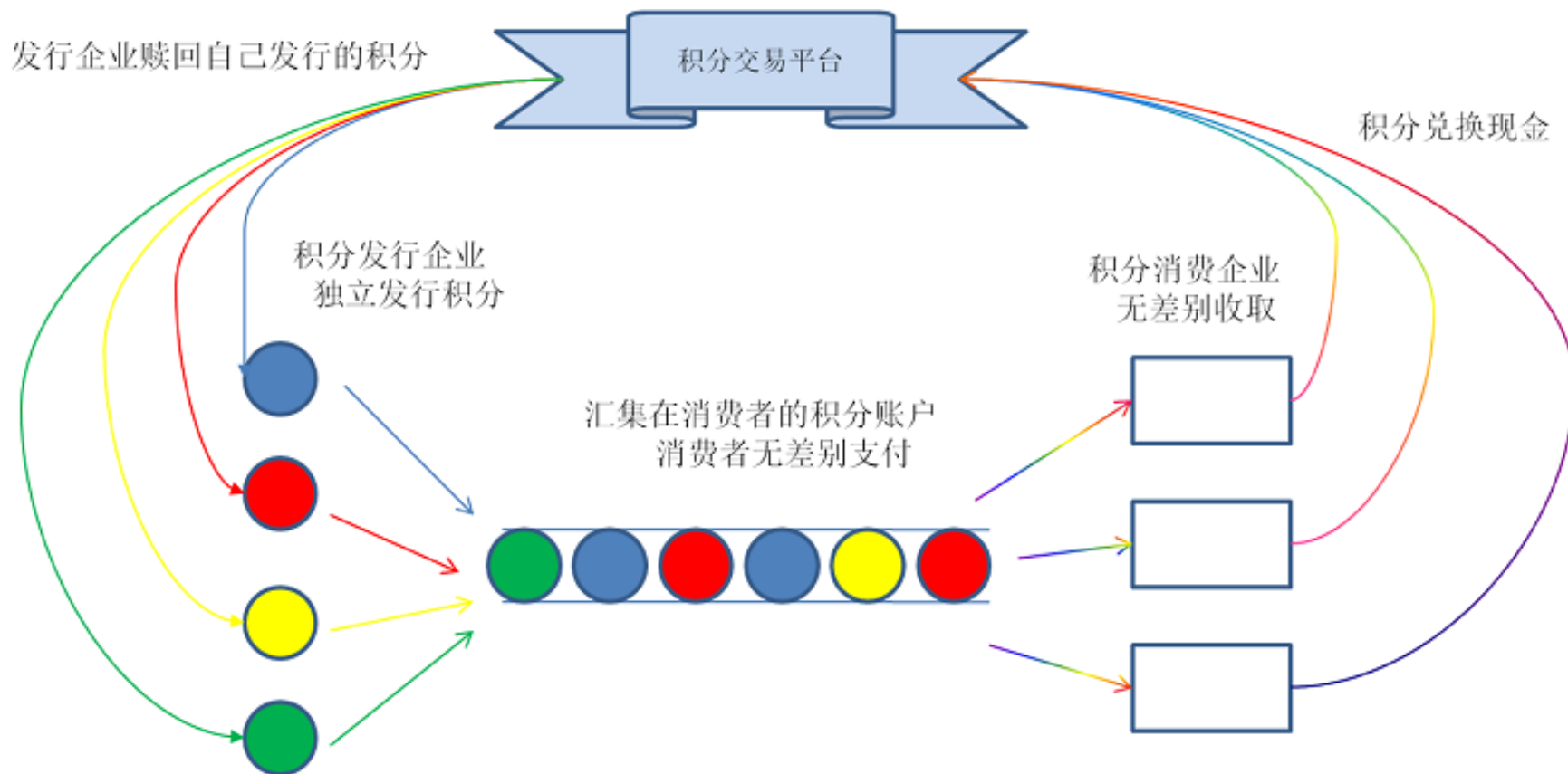


## 去中心化通用积分的原理



构建一个**去中心化**的网络，网络中各个积分企业都可以跟同一个消费者进行交易，而这些企业之间并**不需要**相互的信任。

## 去中心化通用积分的交易流程



运营机制类似与欧元：欧元区各个国家独立发行“特殊标记”的欧元，但是在消费者和商户流通市场，所有的欧元是无差别的。在银行后台清算时，各个国家对自己发行的欧元承担责任。

# Kaka Point

“积分币” 更名 “咔咔积分”



张蕾

手机/微信

186-010-78890