区块链应用

北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

上次课程内容

1 区块

- Hash算法
- Hash指针
- 梅克尔树
- 区块结构

2 密码

- 密码学
- 公钥密码学
- 公钥管理
- 数字签名

3 共识

- P2P
- 分布共识
- 比特币共识
- 隐性共识

4 挖矿

- 矿工任务
- 有效区块
- 激励机制
- 矿机矿池

上次课程内容

技术驱动金融

1 加密货币

- 货币
- 贪心货币
- 财奴币
- 去中心化

2 运行机制

- 脚本
- 网络
- 存储
- 威胁

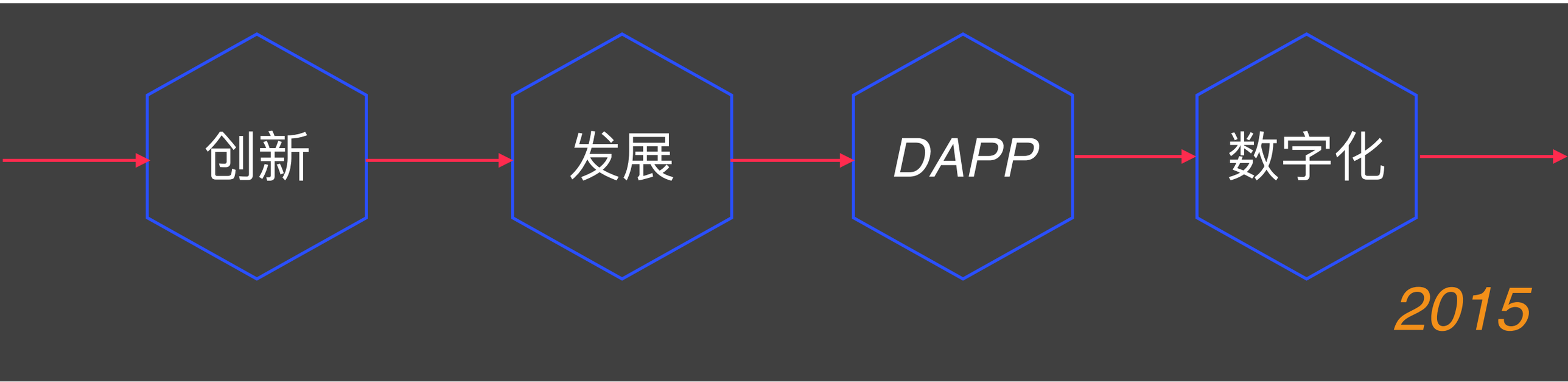
3 监管

- 共识
- 分叉
- 政府态度
- 丝绸之路

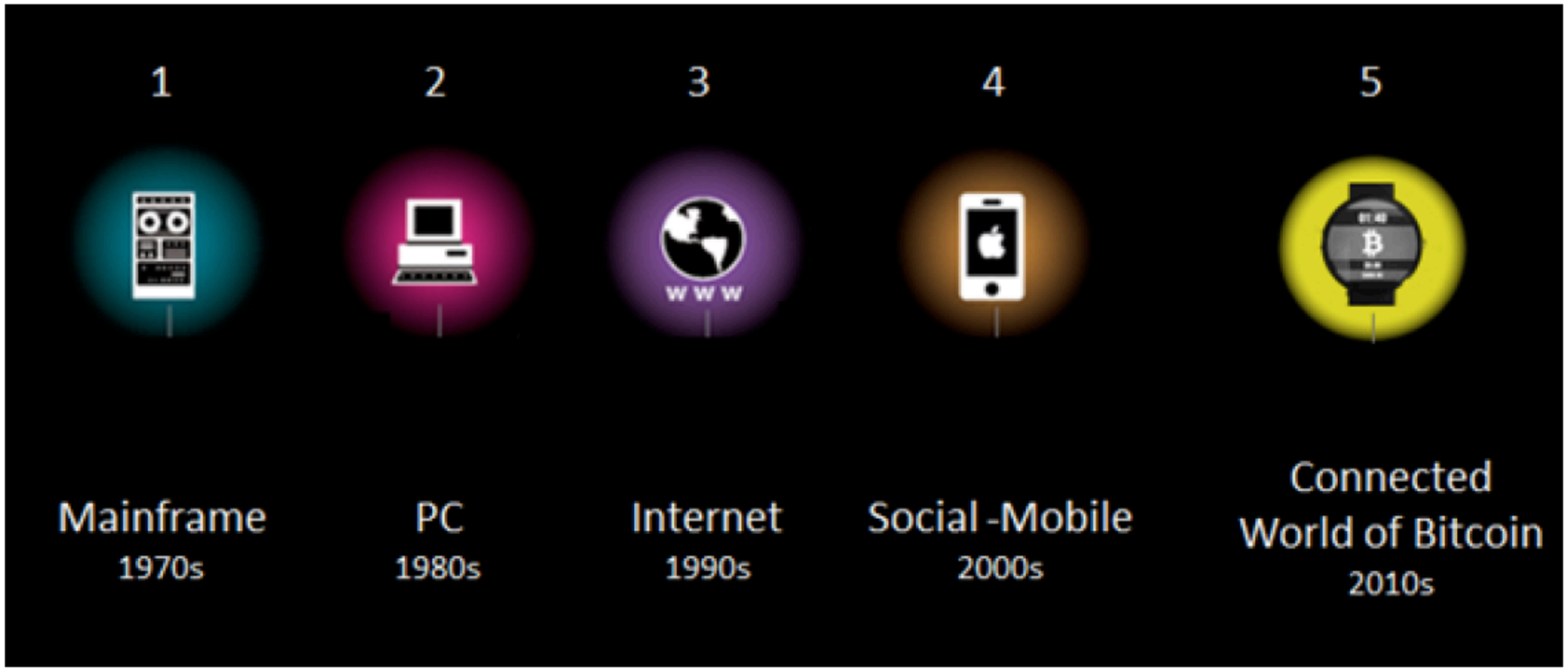
4 匿名

- 定义
- 币的匿名
- 为什么
- 混币

Blueprint for A New Economy



颠覆式创新


1
2
3
4
5
Mainframe
1970s
PC
1980s
Internet
1990s
Social -Mobile
2000s
Connected
World of Bitcoin
2010s

Blockchain Application

区块链+是互联网+一部分

数字化

网络化

智能化

有形资产：汽车、住宅、食品

无形资产：选票、创意、信誉、健康信息

记录、追踪、监测、转移所有资产

政治

文化

智能手机

智能家居

智能汽车

智能城市

可穿戴设备

物联网传感器

自我跟踪设备

Blockchain Application

区块链存证和资产上链

一般	托管交易、保税合同、仲裁、多方签名、...
金融交易	股票、私募、集资、基金、债券、年金、...
公共记录	产权证、车辆登记、营业执照、结婚证、...
证件	驾驶证、身份证、护照、选民登记、...
私人记录	借据、贷款合同、投注、签名、遗嘱、...
证明	保险证明、证权属明、公证文件、...
实物资产	家宅、酒店客房、汽车租赁、汽车使用、...
无形资产	专利、商标、版权、订位、域名、...

DAPP

自治、自足
去中心化

数字资产

DAC

智能合约 → DAPP → DAO → DAS

OpenBazaar　LaZooz　Twister　Storj　Bitmessage

Craigslist　Uber　Twitter　Dropbox　短信

Blockchain Application

区块链3.0

Github+ Bitcoin

NameCoin

BitShares

婚姻 护照

民主 选举

CMUCoin

MitCoin

管理 → DID 数字身份 → BG 区块链政府 → BS 区块链社会

oneName

BitID

BitHandle

病毒管理 公共卫生

学术出版 慈善捐赠

在线学习 健康管理

助力数字化转型

数字化转型：采用数字技术改进服务流程和商业模式

- 个人
- 企业
- 行业
- 政府
- 社会

- 数字化转换
  非数字
- 数字化升级
  新技术

- 信息
- 数据
- 网络
- 智能
- 价值

- 数字技术
- 数字竞争
- 数字客户

IDC预测

2020-2023全球数字化转型投资7.4万亿美元

2023年ICT中投资50%以上是数字化转型

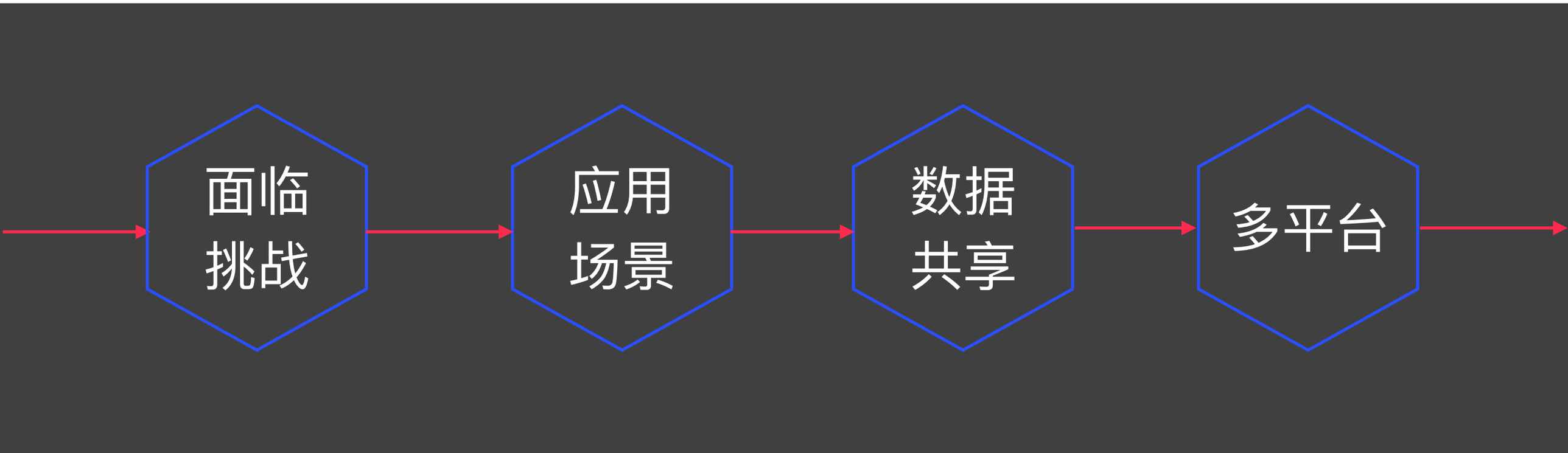
- 数字资源
- 组织结构
- 策略目标

数字经济

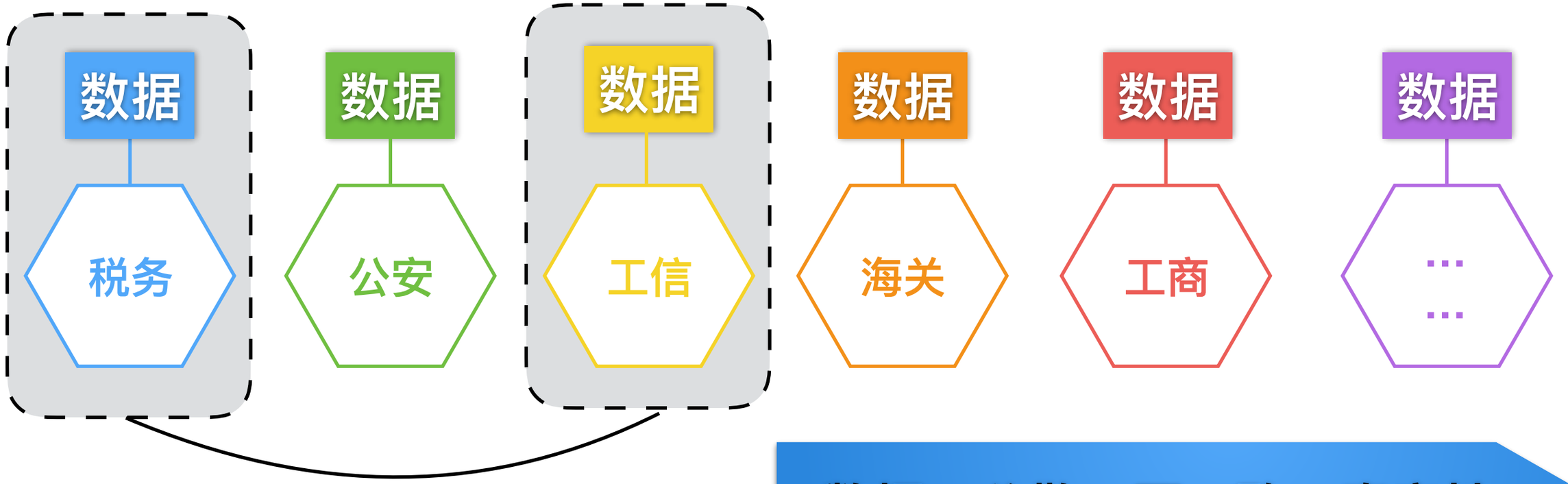
基于数字货物和服务的商业模式，经济收益主要由数字化技术带来的经济形式。

区块链应用逻辑

>>> 以机动车业务为例 <<<

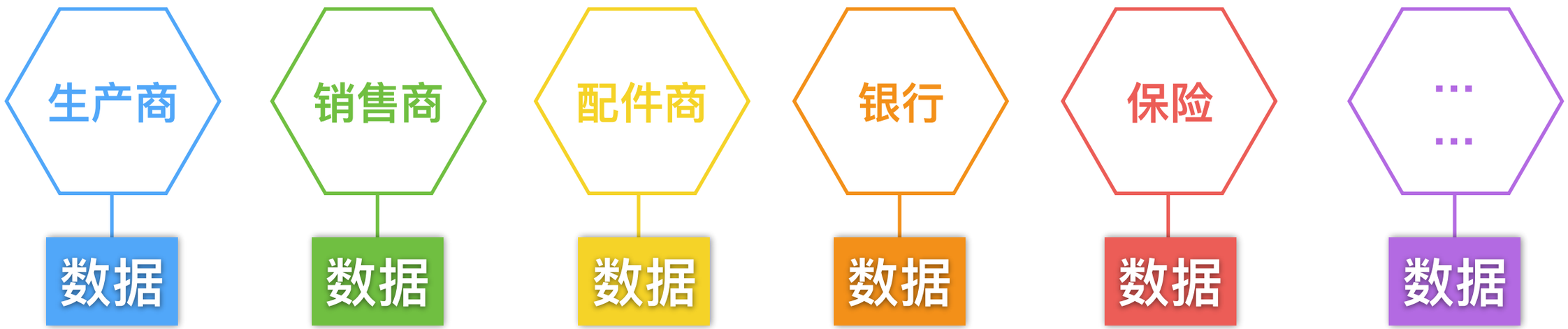


机动车业务面临挑战



数据：分散、不一致、真实性

流程：复杂、跨部门、人工处理

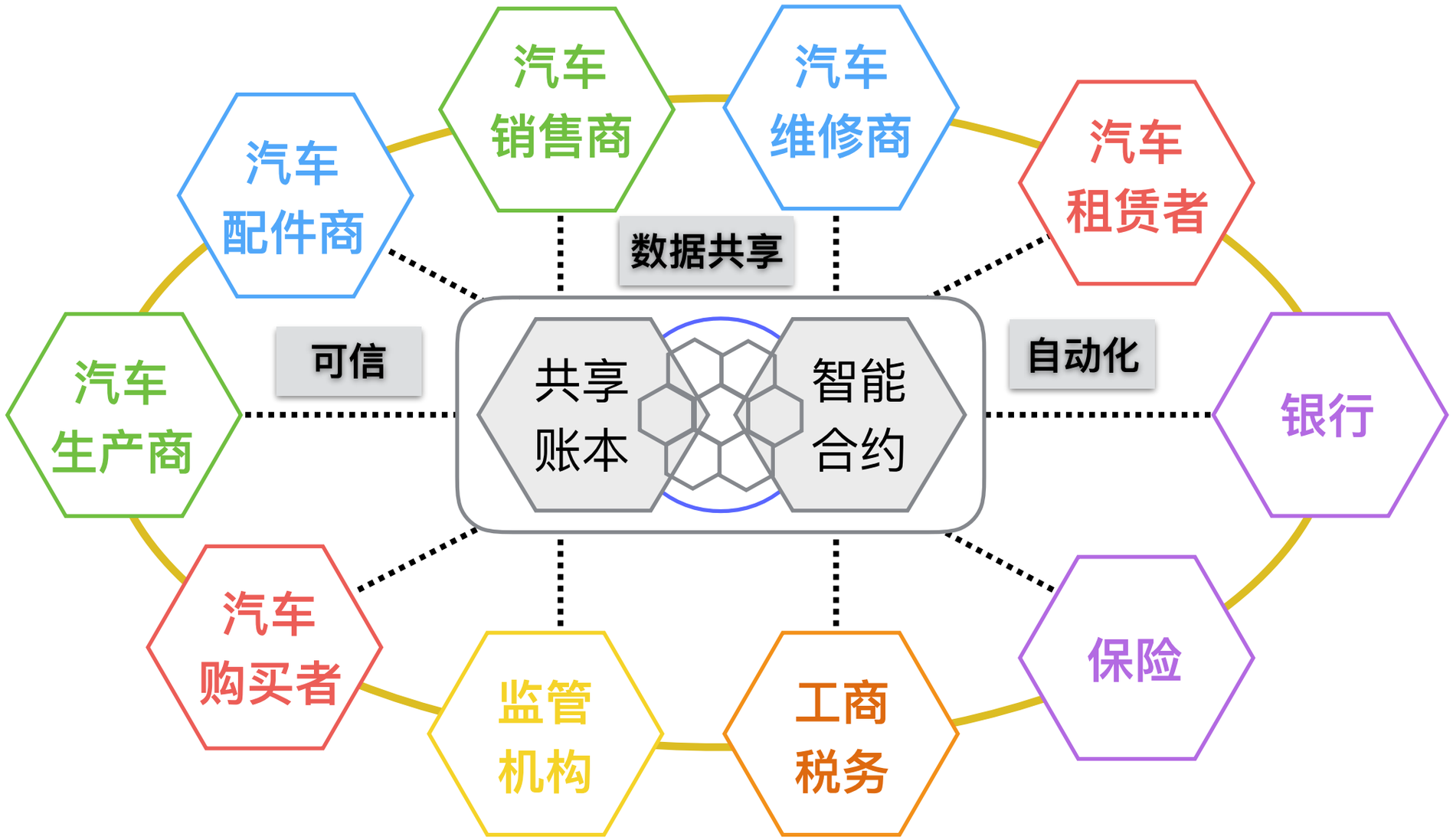


Blockchain Application

区块链应用场景

数据一致性

全生命周期管理

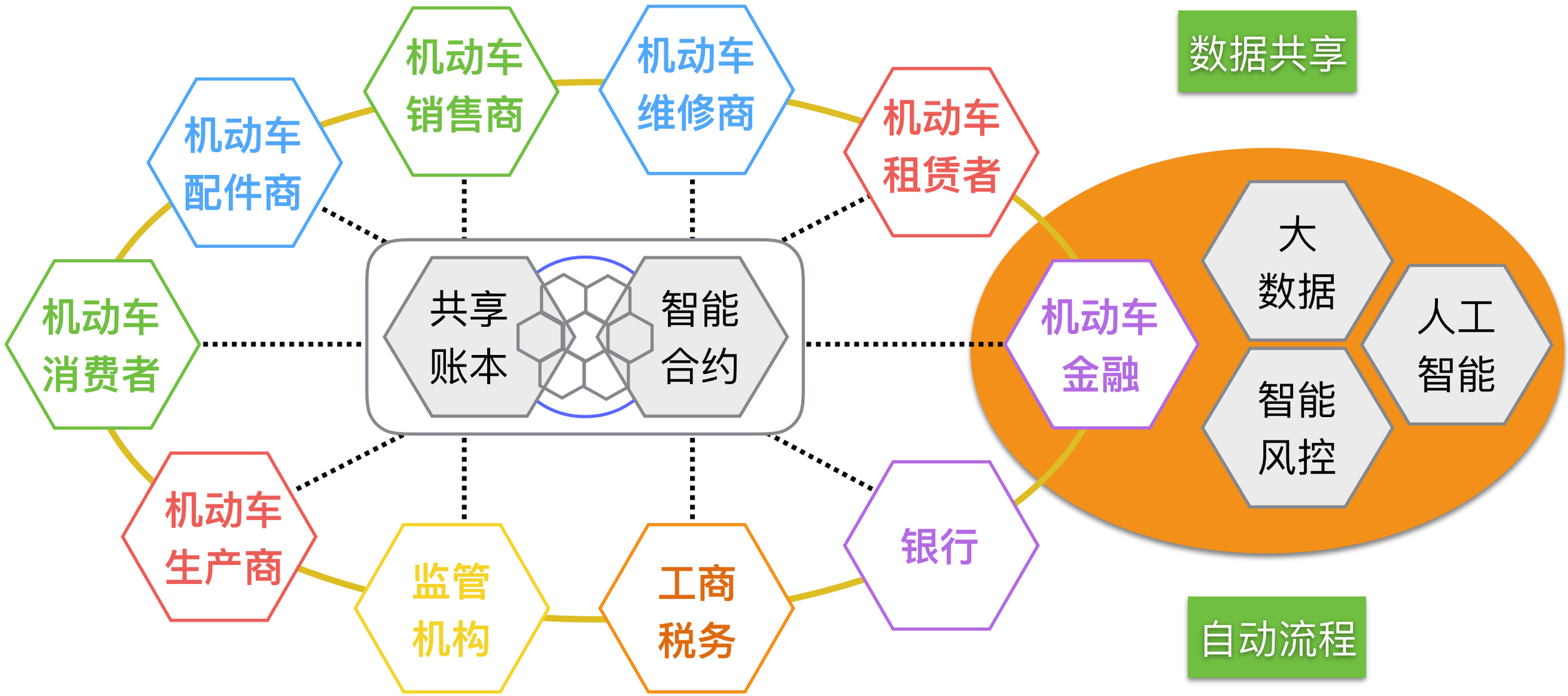


多中心

区块链增信

Blockchain Application

区块链->>防欺诈



基于多来源数据比对防欺诈

基于自动化和智能合约防欺诈

Blockchain Application

区块链->>数据分享平台

机构和人员注册认证

注册 | 认证 | 权限

机动车数据采集

Web | App | 共享

GPS | OBD | 车联网 | IoT | 手机 | 专用

机动车配件商

机动车销售商

机动车维修商

机动车租赁者

机动车消费者

共享账本

智能合约

保险公司

机动车生产商

监管机构

工商税务

银行

金融增值 | 数据增值 | 按需计费 | 名单共享

人员 | 车辆 | 物流 | 资金

联盟链

机动车数据分析

欺诈分析 | 价格分析 | 车辆分析 | 人员分析

机动车数据上链

Blockchain Application

区块链->>其余系统

机构和人员注册认证

注册

认证

权限

机动车数据采集

Web

App

共享

GPS

OBD

车联网

IoT

手机

专用

业务平台

物流

数据采集平台

金融增值

数据增值

按需计费

名单共享

数据集市

智能风控

支付平台

O2O

IOT

大数据平台

区块链平台

人员

车辆

物流

资金

机动车数据分析

联盟链

机动车数据上链

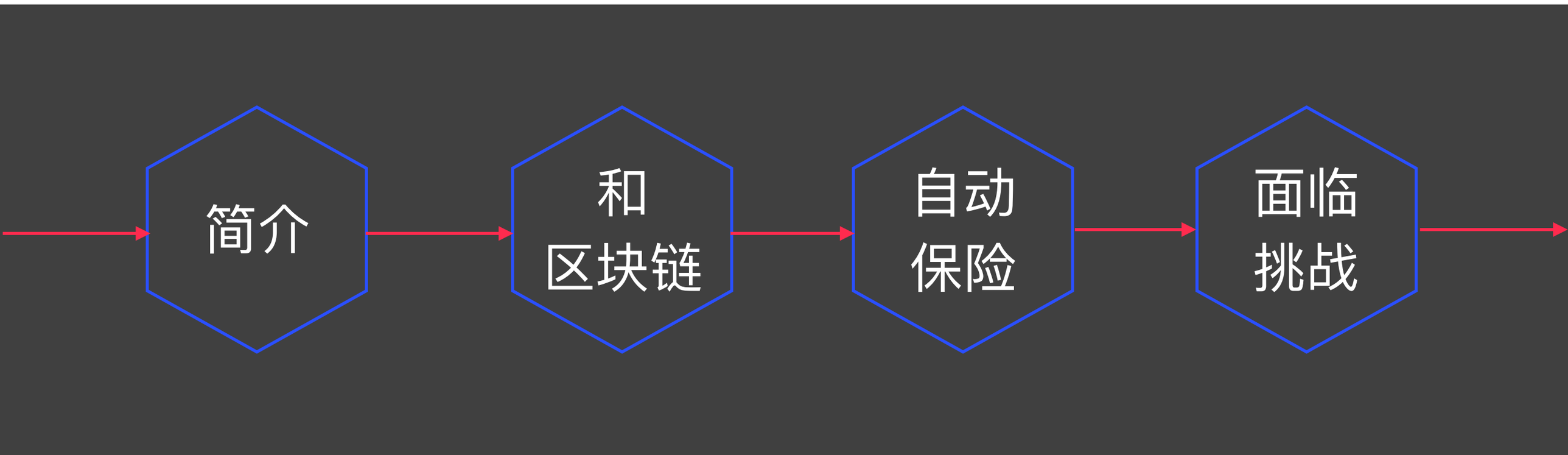
欺诈分析

价格分析

车辆分析

人员分析

智能合约



Blockchain Application

智能合约简介

一组数字形式描述的承诺

包括合约参与方可以执行这些承诺的协议

Nick Szabo 1990

以太坊 2013

实际合约 | 部分合约 | 非合约

规则逻辑 | 软件代码 | 自动执行

身份标识 | 系统状态 | 发生事件

Blockchain Application

智能合约和区块链

自动执行

非区块链智能合约

- 参与方认证
- 合约协商
- 编码合约
- 状态设定
- 合约发布
- 合约上链
- 合约更新
- 合约执行

智能合约在区块链上存储并执行

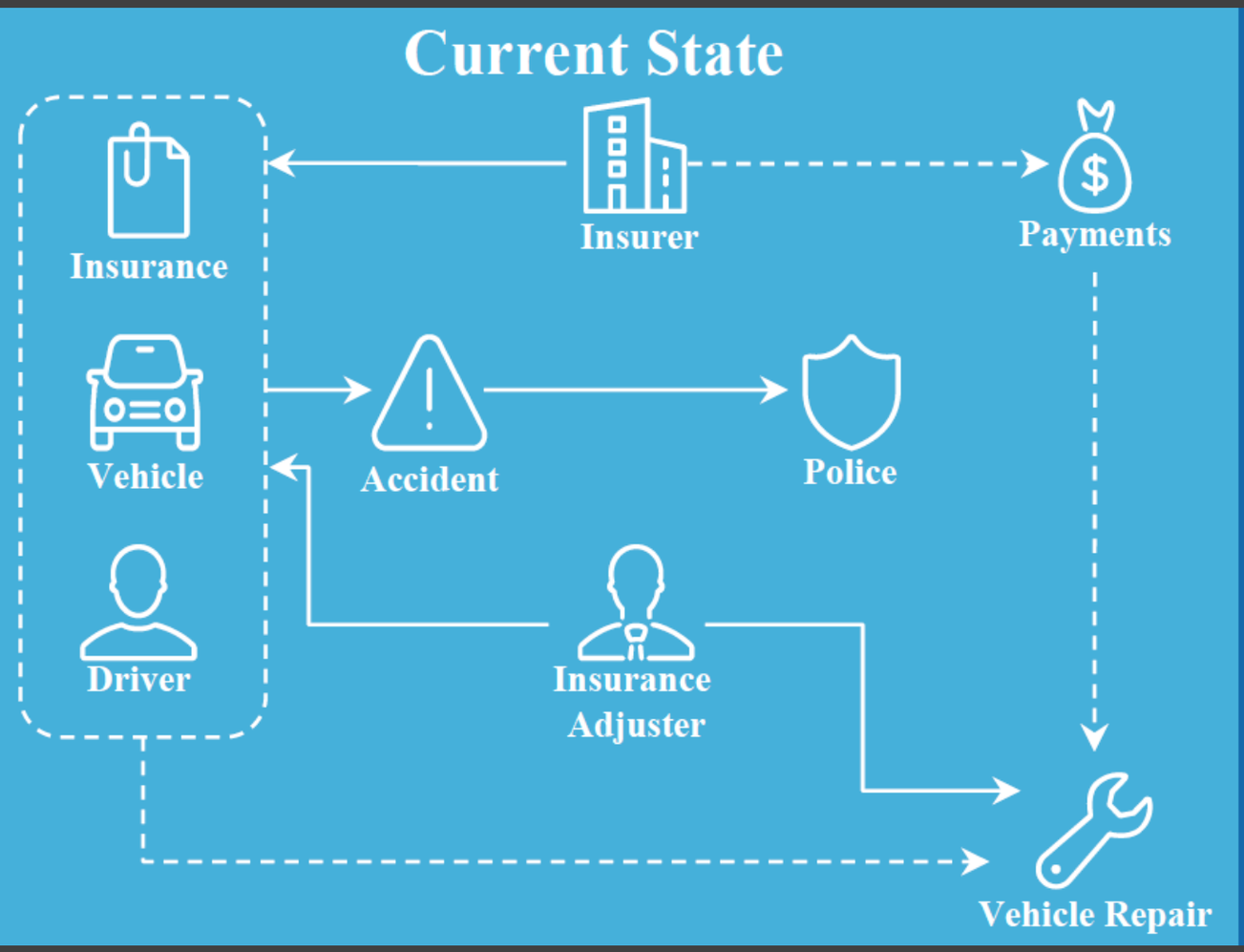
Block #FCAC
prev #618C
</> contract 2E12…
</> contract FECB…
</> contract 21E0…
…

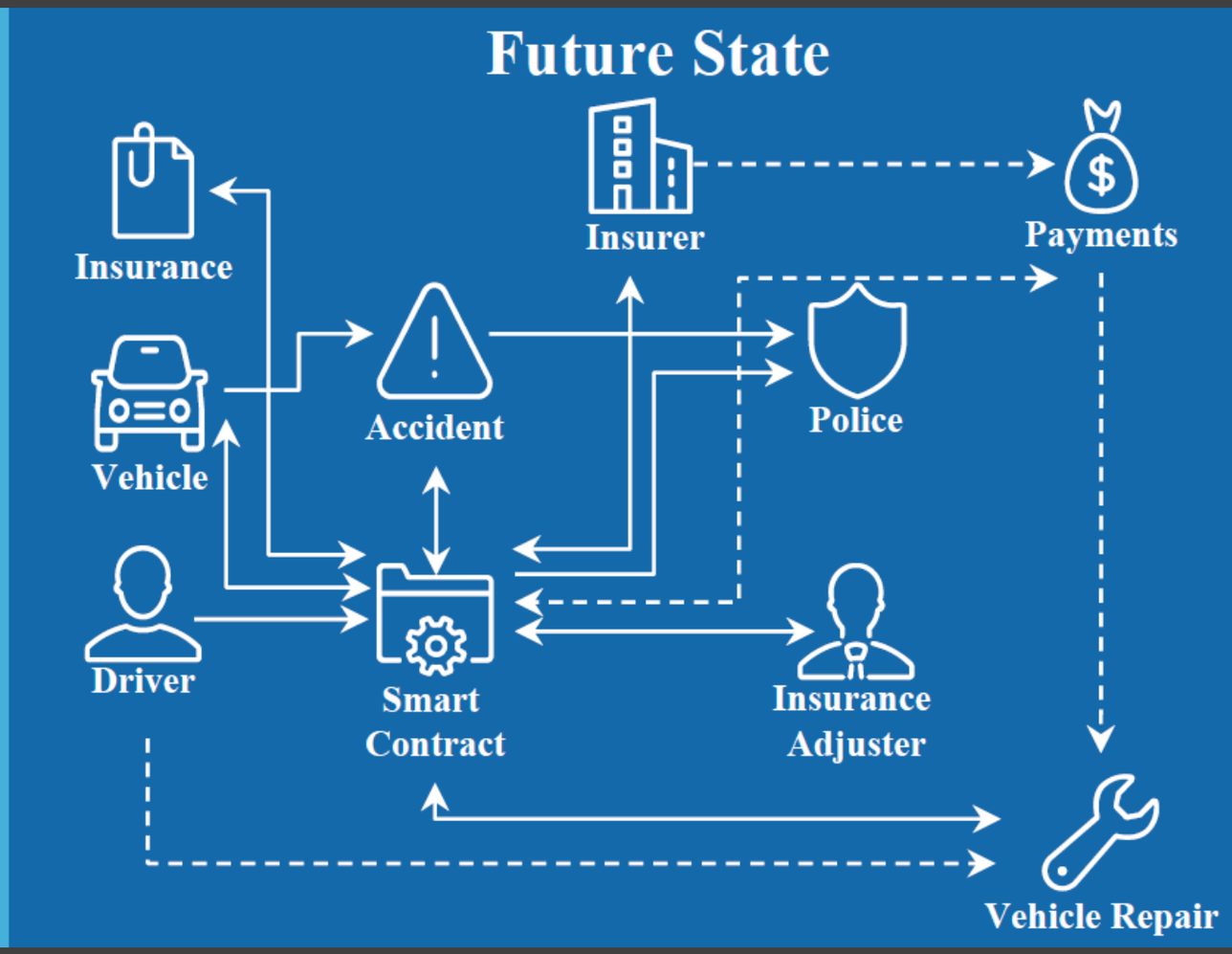
Block #51E5
prev #FCAC
</> contract 0EBF…
</> contract 7B4E…
</> contract 3390…
…

Block #
prev #
</> con
</> con
</> con
…

Blockchain Application

智能合约应用案例 - 自动保险





P2P保险

指数保险

多方保险

资产管理

智能合约面临挑战

操作风险

- 缺乏有效的后备和故障切换机制
- 有时候依赖其余系统来履行合约
- 智能合约平台有可能存在问题
- 区块链存在硬分叉可能性

技术风险

- 任何软件都存在漏洞
- 人是会犯错误
- 网络、计算机、服务器风险
- 外部预言机失败、崩溃

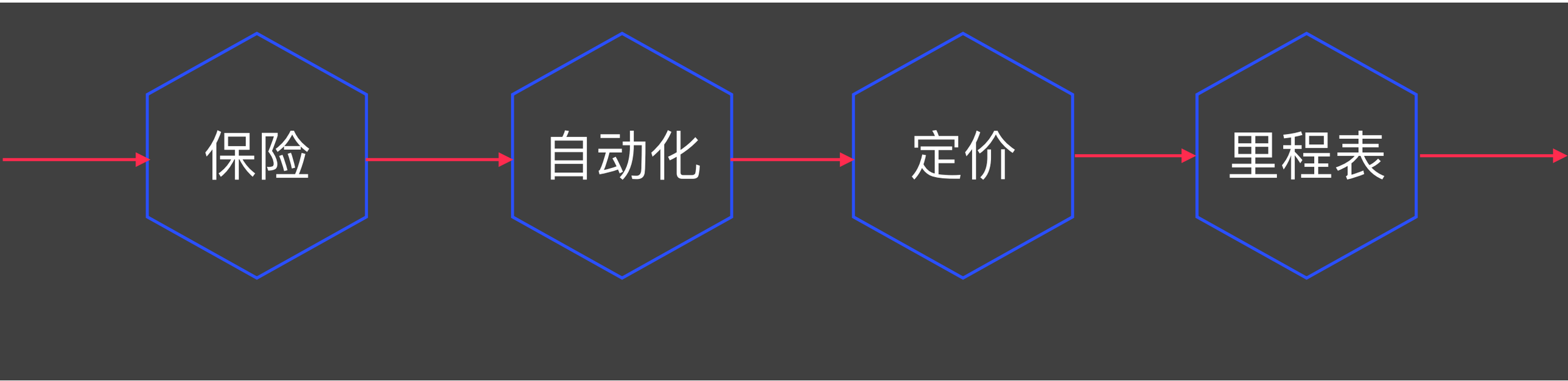
安全

- 智能合约执行的正确性判断
- 智能合约的安全性
- 相关系统的安全性
- 外部预言机的安全保证

监管

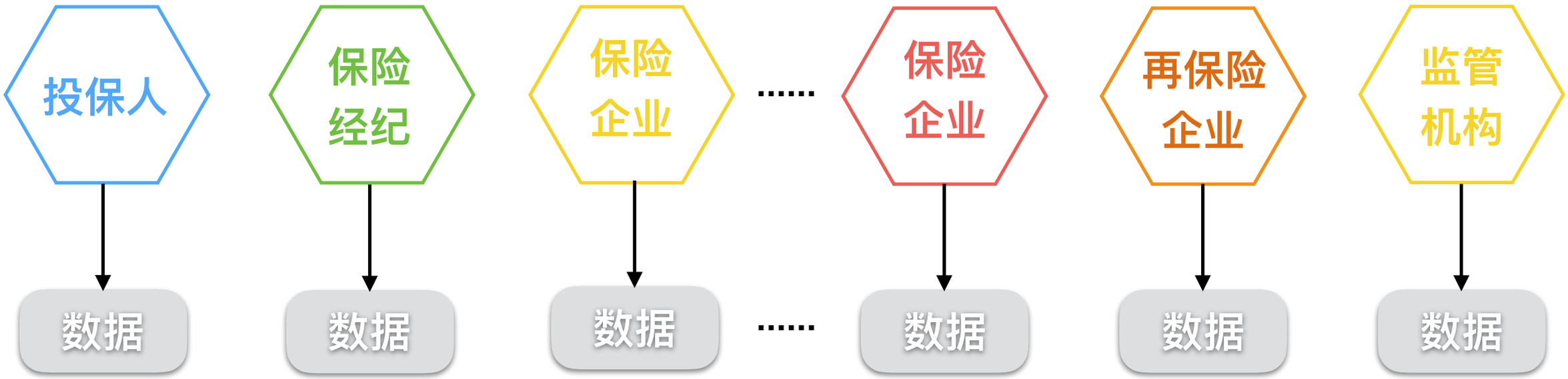
- 智能合约也可能包括不合法代码
- 内部人可以操控智能合约
- 智能合约实际执行和宣传不符
- 外部预言机被操纵

保险应用



Blockchain Application

保险



核保

核损

定价

风控

KYC

防欺诈

人工流程

信息披露

数据孤岛

隐私泄漏

一致性

监管

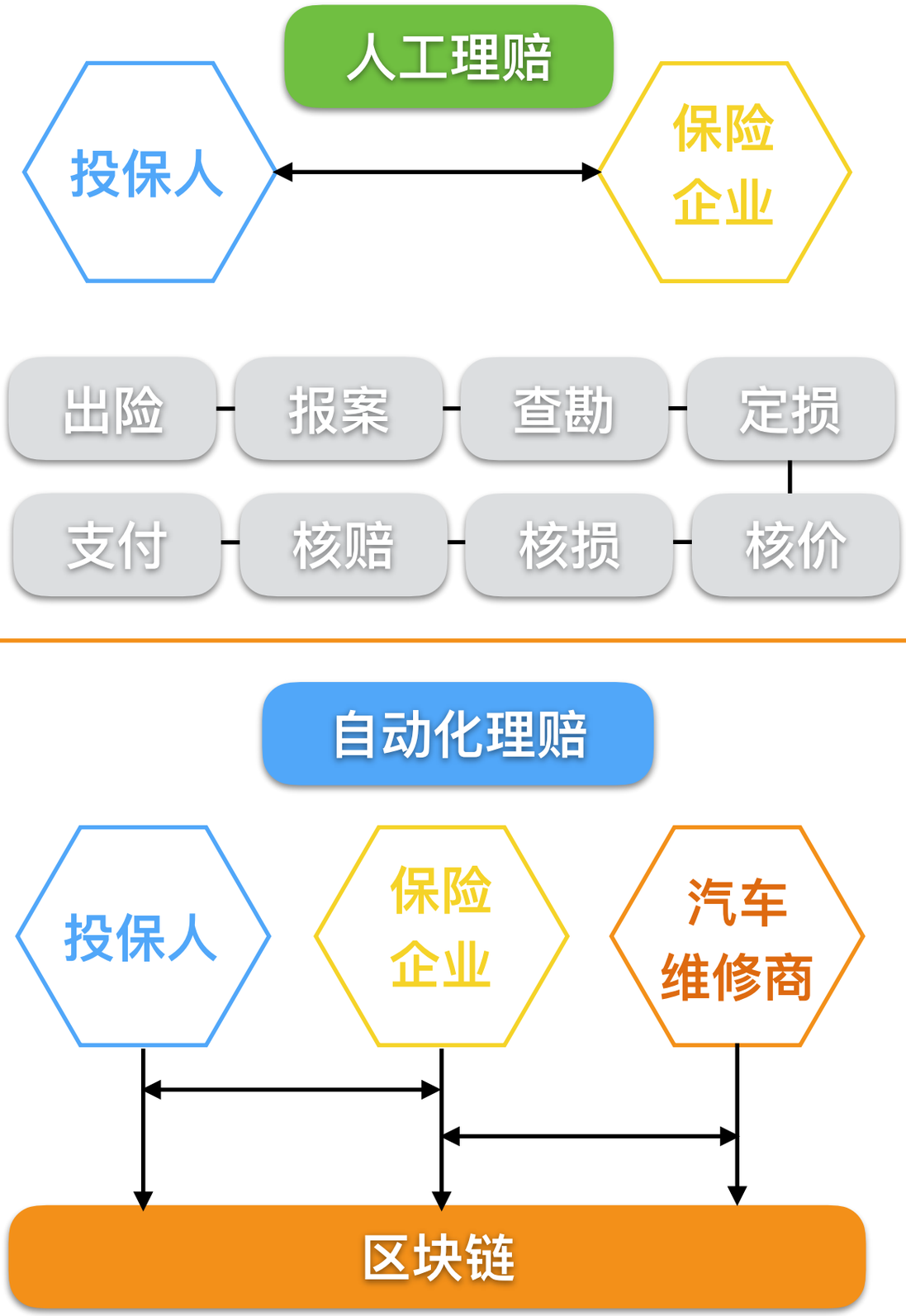
AI

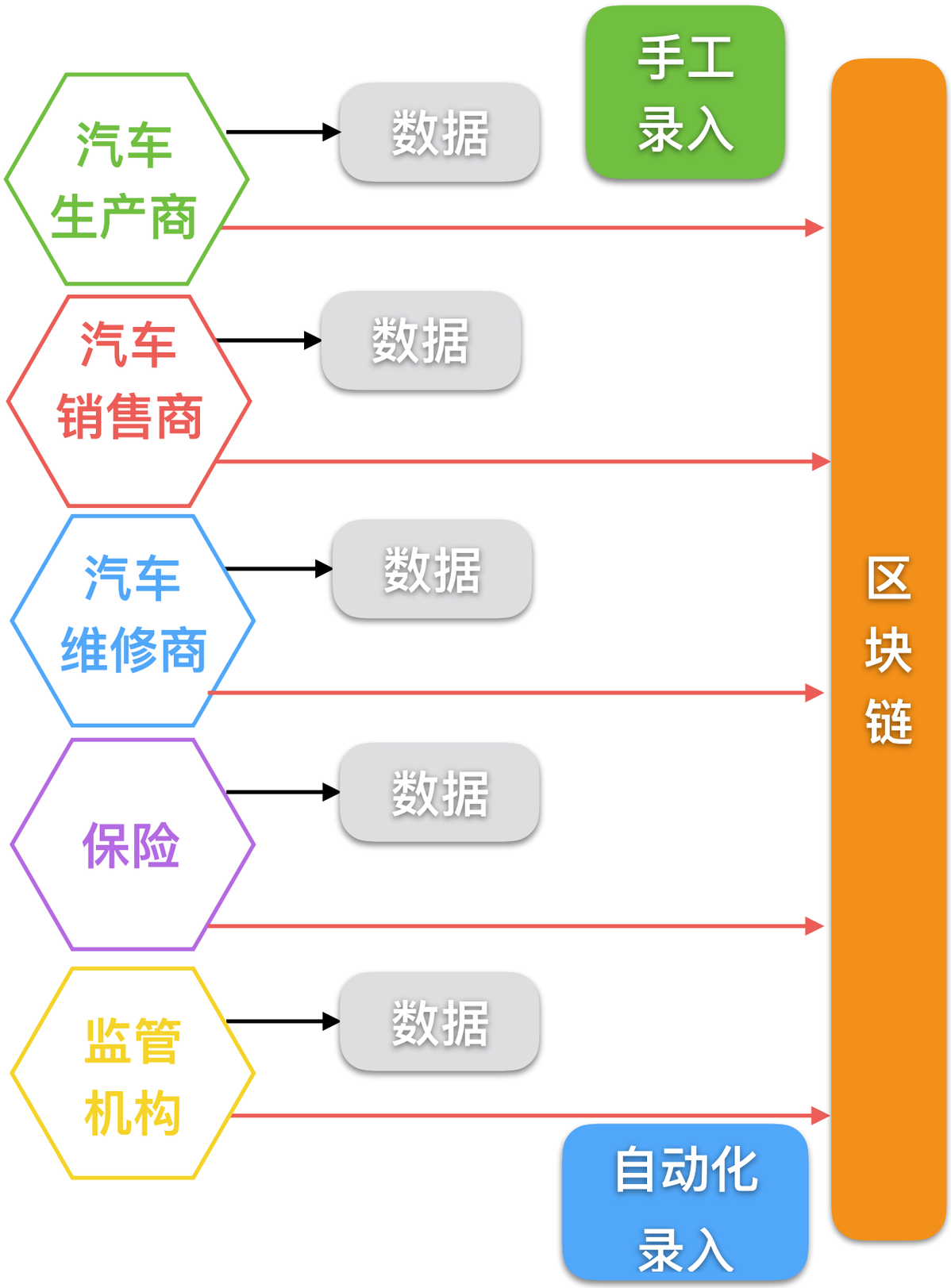
BigData

Cloud

Blockchain

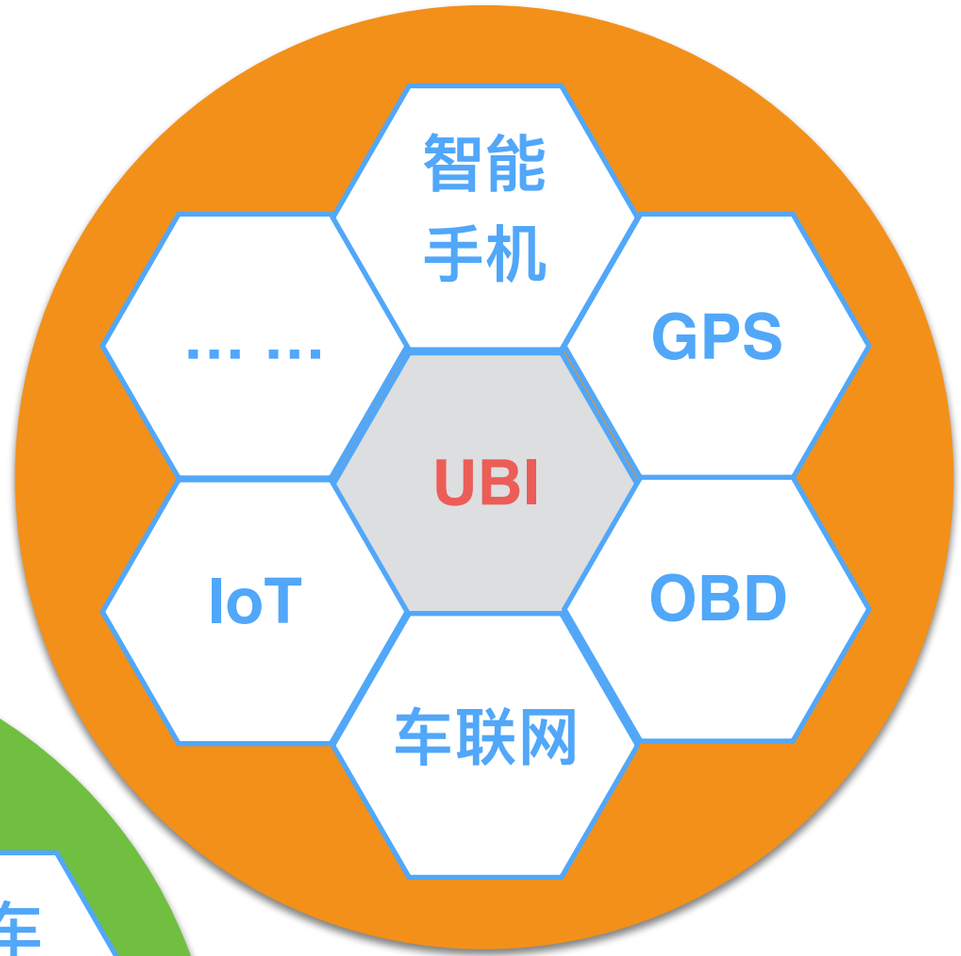
自动化


人工理赔
投保人
保险企业
出险
报案
查勘
定损
支付
核赔
核损
核价
自动化理赔
投保人
保险企业
汽车维修商
区块链


手工录入
汽车生产商
数据
汽车销售商
数据
汽车维修商
数据
保险
数据
监管机构
数据
区块链
自动化录入

定价

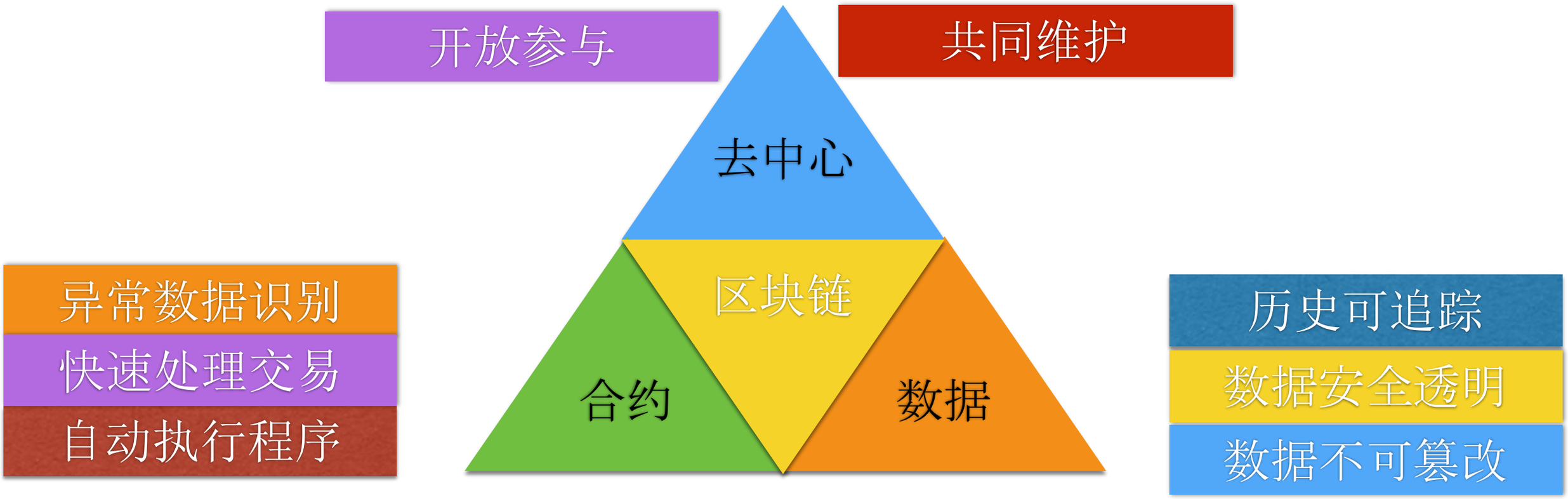

人员
信息
驾驶
信息
车辆
信息
风险
定价
出险
信息
违章
信息
维修
信息


智能
手机
… …
GPS
UBI
IoT
OBD
车联网


智能
车辆
电动
汽车
汽车
共享
MaaS
保险
KYC
汽车
租赁

里程表欺诈


数据上传
数据处理
查询购买
数据下载
交易记录

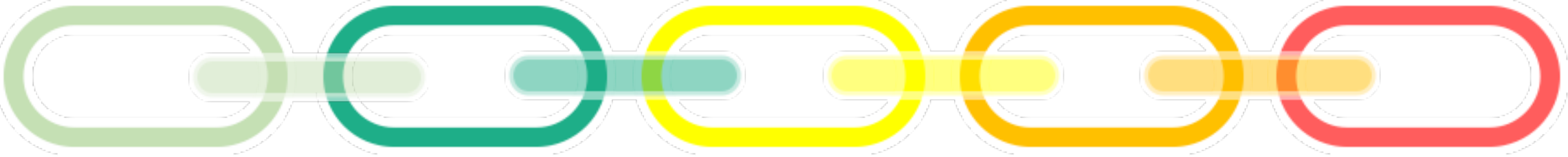

开放参与
共同维护
去中心
区块链
合约
数据
异常数据识别
快速处理交易
自动执行程序
历史可追踪
数据安全透明
数据不可篡改

里程表欺诈

汽车制造商：提交汽车出厂时的详细配置信息，一辆汽车的生命周期的起点数据。

国家车辆登记机关：拥有官方隐私数据，涉及到这些数据需要较高的权限才能获取。

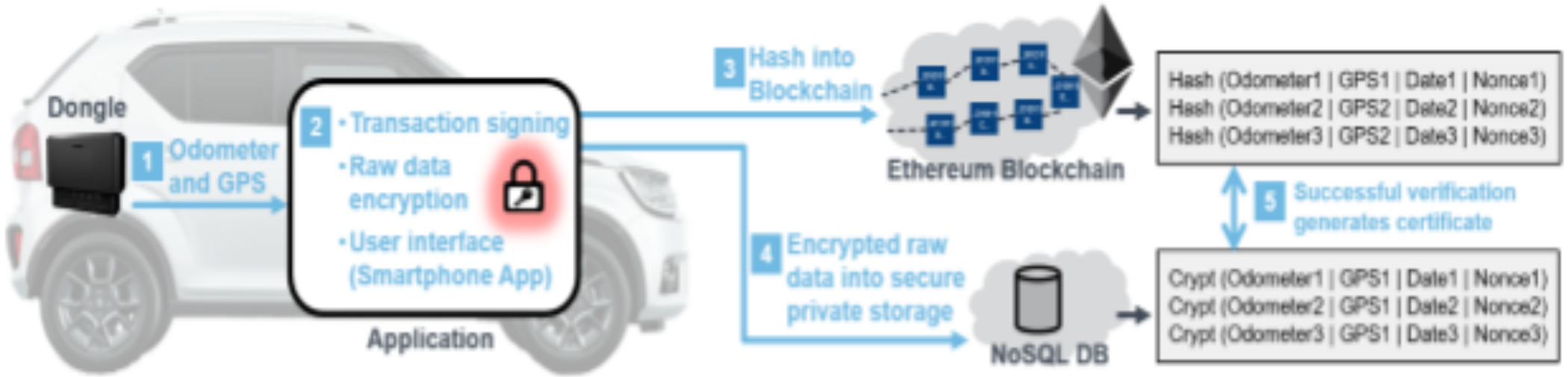
保险公司：保险公司拥有汽车保险信息，以及通过保险理赔的事故信息和维修记录。

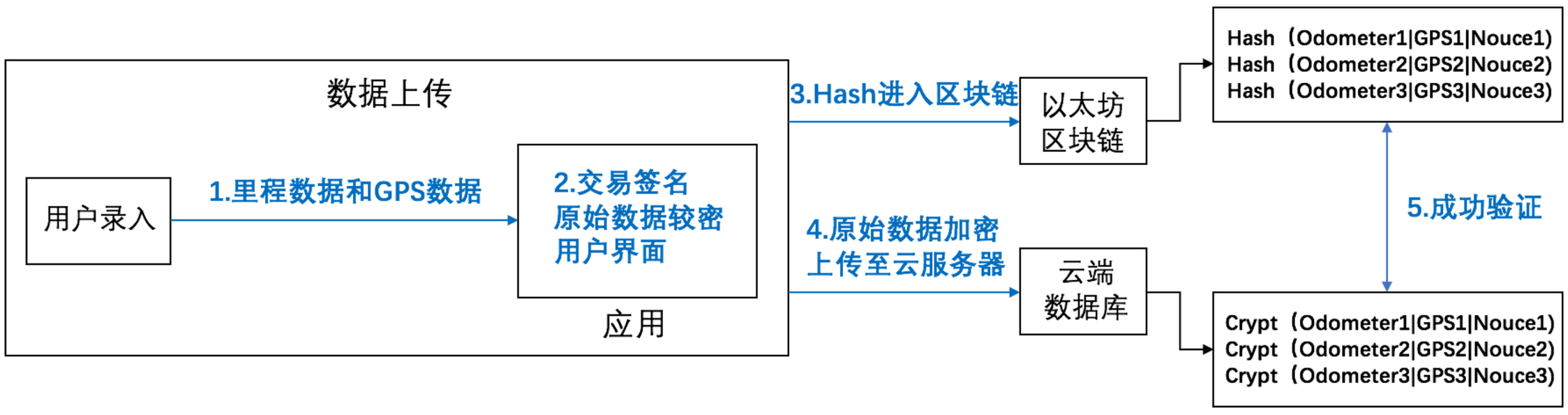


汽车使用者：通过车载远程设备是记录汽车数据，主动规律得上传汽车的使用情况，比如里程、gps、油耗、车速等。或允许用户手动录入。

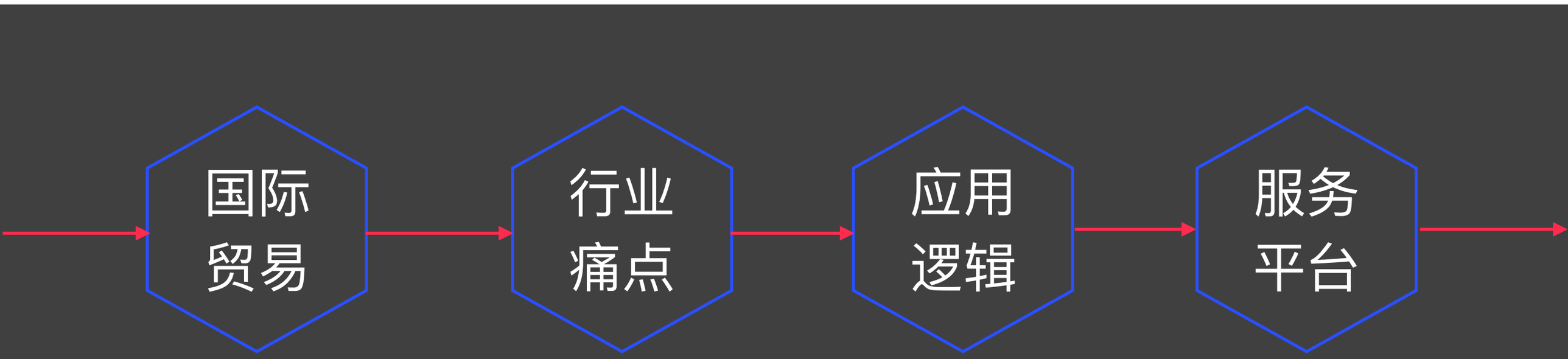
汽车服务商和服务站：汽车在进行维修时，维修站向相关部门提交汽车的数据，汽车服务商收集的数据，可以与其它渠道的数据相互印证。

里程表欺诈


Dongle
1 Odometer and GPS
2 • Transaction signing
• Raw data encryption
• User interface (Smartphone App)
Application
3 Hash into Blockchain
Ethereum Blockchain
Hash (Odometer1 | GPS1 | Date1 | Nonce1)
Hash (Odometer2 | GPS2 | Date2 | Nonce2)
Hash (Odometer3 | GPS2 | Date3 | Nonce3)
4 Encrypted raw data into secure private storage
NoSQL DB
5 Successful verification generates certificate
Crypt (Odometer1 | GPS1 | Date1 | Nonce1)
Crypt (Odometer2 | GPS1 | Date2 | Nonce2)
Crypt (Odometer3 | GPS1 | Date3 | Nonce3)


数据上传
用户录入
1.里程数据和GPS数据
2.交易签名
原始数据较密
用户界面
应用
3.Hash进入区块链
以太坊
区块链
4.原始数据加密
上传至云服务器
云端
数据库
Hash（Odometer1|GPS1|Nouce1)
Hash（Odometer2|GPS2|Nouce2)
Hash（Odometer3|GPS3|Nouce3)
5.成功验证
Crypt（Odometer1|GPS1|Nouce1)
Crypt（Odometer2|GPS2|Nouce2)
Crypt（Odometer3|GPS3|Nouce3)

国际贸易应用



Blockchain Application

国际贸易

进口 协会 平台 出口

代理 物流 承运 港口

银行 保险 基金 投资

海关 税务 外汇 商检

行业痛点

流程时间长

对于出口商，从境外合同签订到最终交付，出口核销完成，一般中小企业需要2-3个月时间；

中间成本高

从合同签订到完成出口涉及众多中间环节，各个环节中均有费用产生，中间成本高，帐期长；

监管不便利

涉及中间环节多，为不法分子提供了可乘之机，出口骗税案件涉案金额大；

信息不透明

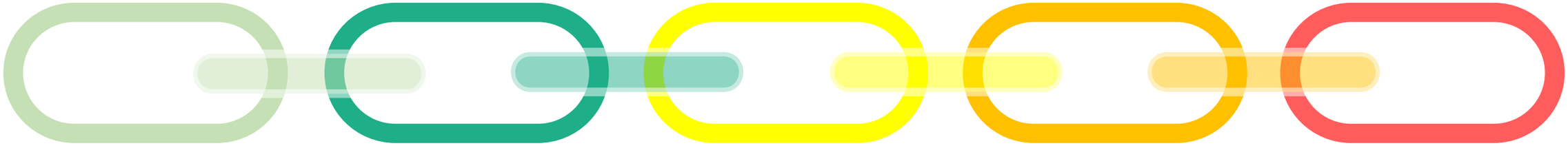
涉及环节多，中间只靠纸质单据流转，信息极度不透明；

Blockchain Application

应用场景

使用区块链来更新改造传统的外贸信用证、外贸保函、福费廷、保理和票据等业务。

使用联盟链多方参与的特性链接海关、税务、商检、外汇等管理机构，加快国际贸易流程，提高监管水平。



基于物联网等终端采集设备，采集国际贸易整个供应链上的相关数据，并结合大数据和区块链，保证数据的真实可信。

基于采集到的国际贸易供应链数据，使用专门为国际贸易定制的风控模型和算法，为企业画像，智能评估企业信用，减少欺诈行为，降低风险。

Blockchain Application

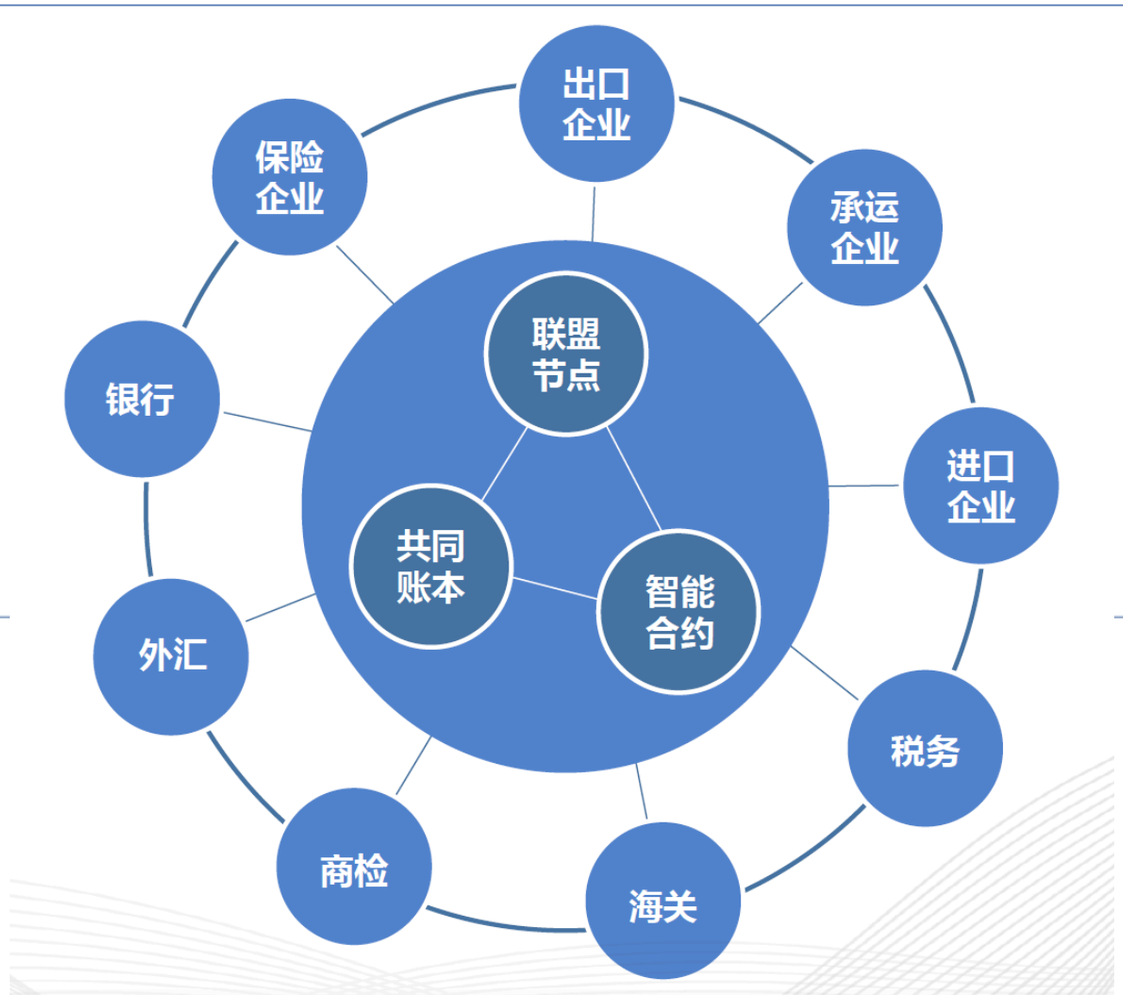
国际贸易服务平台

会员服务 — 信息服务 — 风控服务 — 贸易服务 — 金融服务

区块链

金融科技

大数据



人工智能

物联网

云计算

Blockchain Application

国际贸易服务平台架构

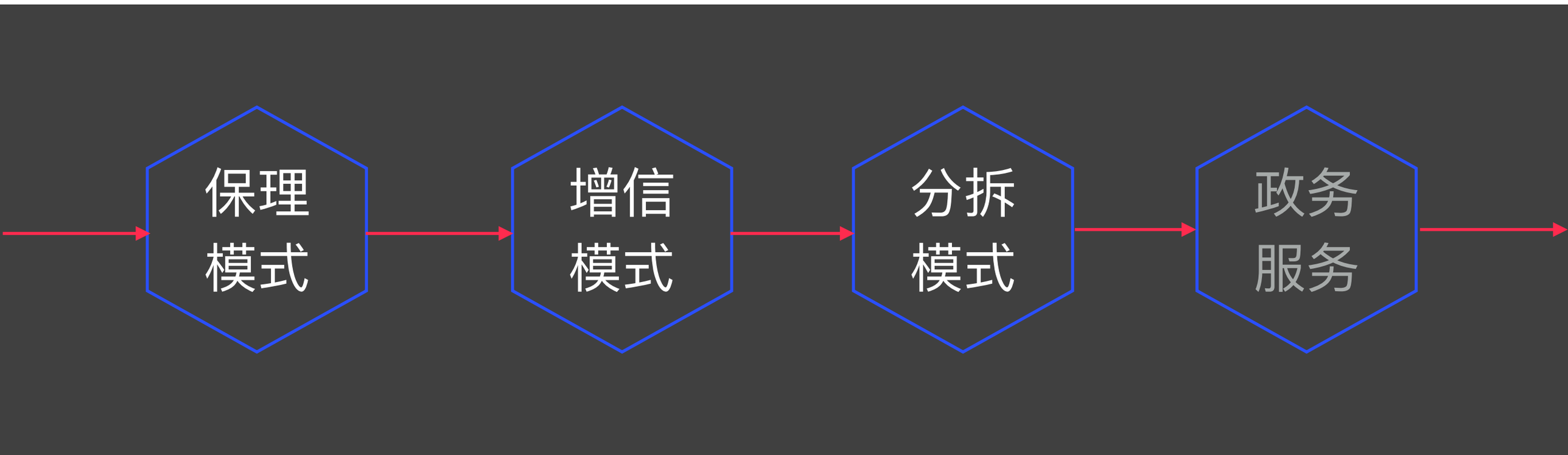
经纪人注册	经纪人交流	经纪人培训	国家专家智库
注册 认证 考核	展会 论坛 产业	贸易 金融 区块链	理事 专家 政策

经纪人合作	政务 通关 财税 保理 征信 物流 结算 仓储 融资 保险	经纪人辅导
标准 研发 协会		理事 专家 政策

数据	画像	报告	模型
海关 税务 银行 征信 宏观 仓储	控制人行业 上下游 成长性 稳定性 历史	初筛 信用 评分 审贷 授信 定制	贷前 贷中 贷后 反欺诈 反洗钱 特殊

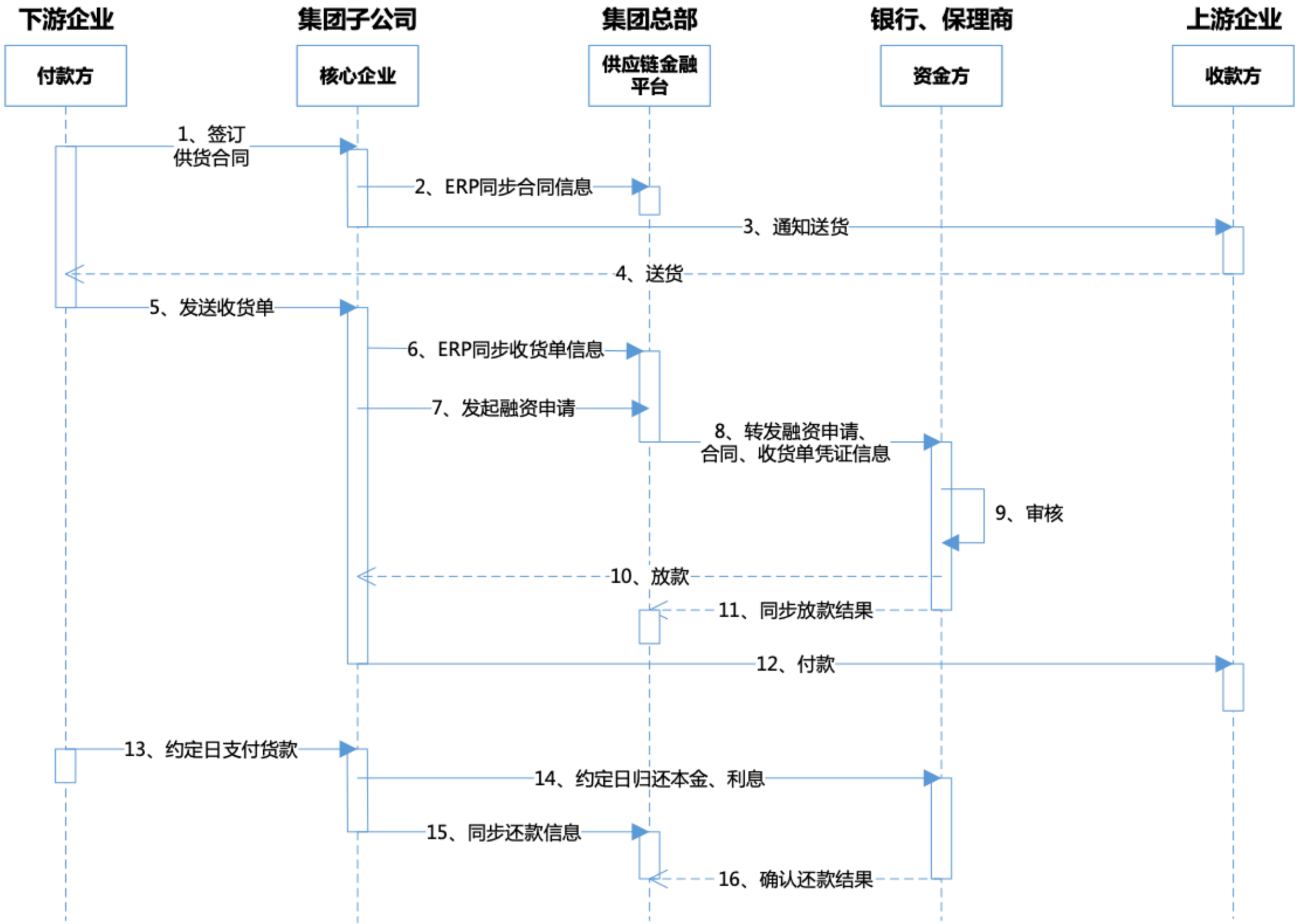
信息来源	信息采集	信息汇报	信息平台
人员 物流 资金 生产 物流 仓储	摄像头 RFID GPS LOT 手机 专用	企业 行业 供应链 政府 金融 第三方	Web APP 特 殊 区块链 大数据 云计算

供应链金融应用

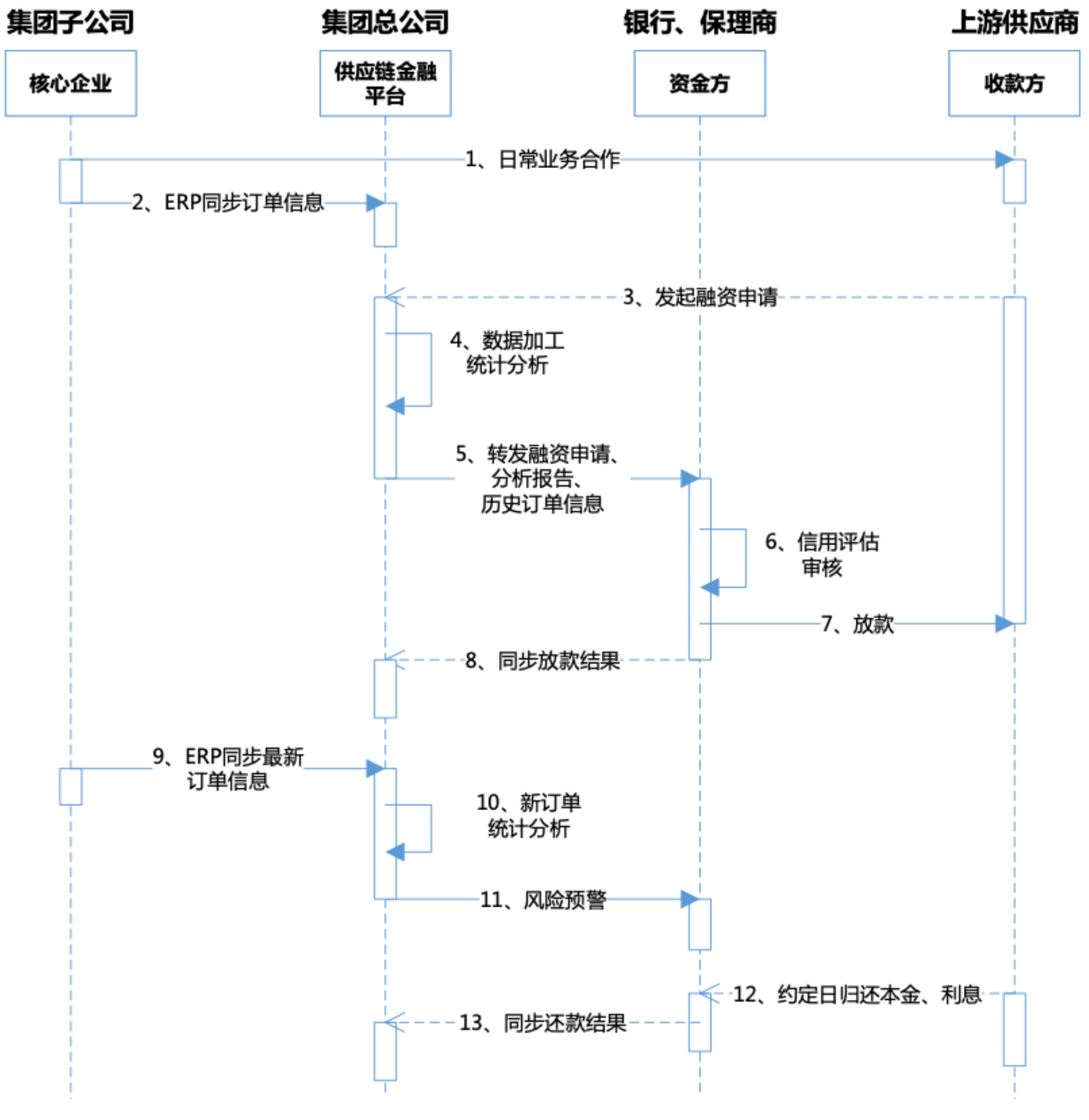


Blockchain Application

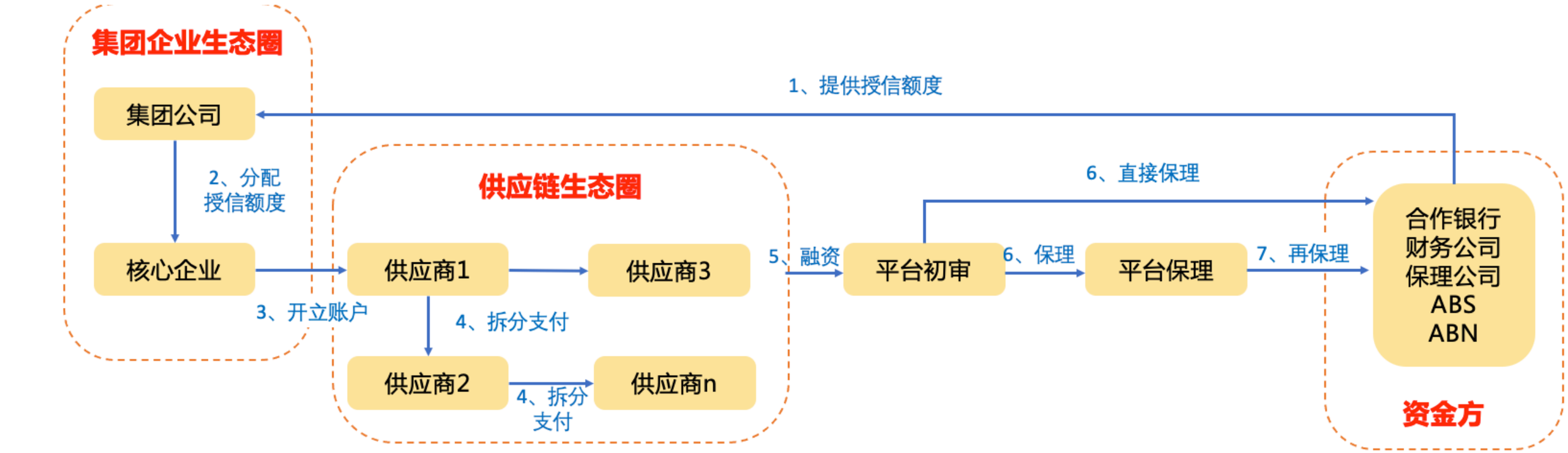
供应链金融-保理模式



供应链金融-增信模式


集团子公司
集团总公司
银行、保理商
上游供应商
核心企业
供应链金融平台
资金方
收款方
1、日常业务合作
2、ERP同步订单信息
3、发起融资申请
4、数据加工
统计分析
5、转发融资申请、
分析报告、
历史订单信息
6、信用评估
审核
7、放款
8、同步放款结果
9、ERP同步最新
订单信息
10、新订单
统计分析
11、风险预警
12、约定日归还本金、利息
13、同步还款结果

供应链金融-区块链赋能



服务

ERP系统对接 | 银行系统外接 | 供应链金融风控 | 核心企业管理 | 供应商管理 | 拆分支付 | 融资

区块链

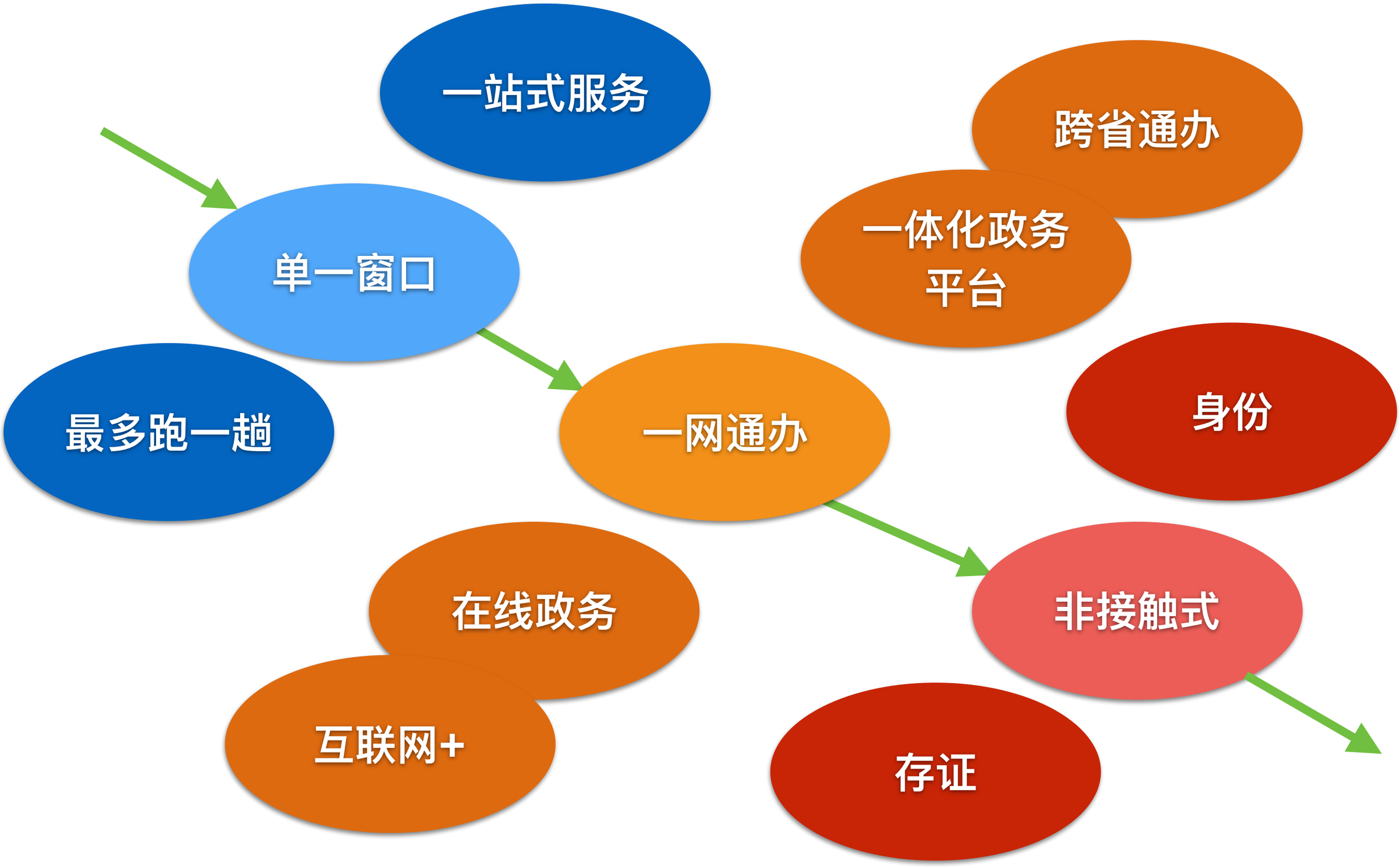
采购 — 物流 — 合同 — 融资 — 仓储 — 报销 — 零售 — 审核 — 监管 — 信用 — 渠道

联盟链

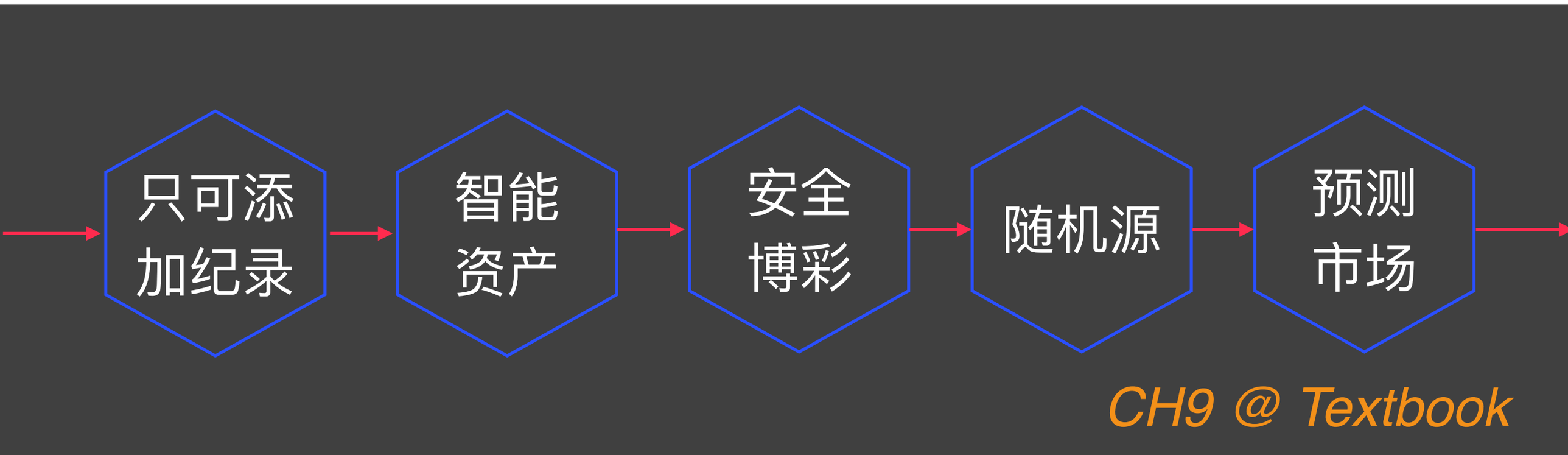
解决票据 | 拆分流转 | 便利支付 | 金额错配 | 账期错配

Blockchain Application

政务服务应用



比特币作为平台



CH9 @ Textbook

比特币平台

- 比特币已经work，基于比特币能做什么？

- 作为一个只能增加的记录
- 作为一个智能资产
- 建立博彩系统
- 建立公共随机数源
- 建立预测市场

安全时间戳

- 时间TI公布H(r, x)，TI后可以公布r和x

时间戳　　Hash指针　　安全时间戳

- 证明创意的有限性
- 证明一些事件的先后顺序

版权登记的区块链应用　　电子证据　　面临挑战

Blockchain Application

预测未来

TWEETS 5 | FOLLOWERS 3,925 | More

Tweets | Tweets and replies

FIFA Corruption @FifNdhs · 17h
There will be a goal in the second half of ET
17K 3.3K

FIFA Corruption @FifNdhs · 17h
Gotze will score
19K 3.8K

FIFA Corruption @FifNdhs · 17h
Germany will win at ET
17K 3.4K

FIFA Corruption @FifNdhs · 17h
Tomorrows scoreline will be Germany win 1-0
18K 3.6K

FIFA Corruption @FifNdhs · 17h
Prove FIFA is corrupt
15K 2.7K

FIFA2014

腐败指责

FIFA Corruption @fifndhs
Germany will win at ET
17 hours ago Reply Retweet Favorite 12K more

FIFA Corruption @fifndhs
Argentina will win in penalties
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs
Gotze will score
17 hours ago Reply Retweet Favorite 14K more

FIFA Corruption @fifndhs
There will be a goal in the second half of ET
17 hours ago Reply Retweet Favorite 12K more

FIFA Corruption @fifndhs
Kroos will score
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs
Lahm will score
17 hours ago Reply Retweet Favorite

FIFA Corruption @fifndhs
Palacio will score
17 hours ago Reply Retweet Favorite

离线时间戳


26
guardtime
guardtime.com
15 July 2009 00:00:00 UTC
AAAAAA-CKLUOA-AAI7FX-EKPAMP
VRUBSC-7DQE7O-TZBCP4-MS5S65
UEOSEC-UU2A3N-OCCCIR-PLM4PG
Friday July 17 2009
S&P 500 index
1000
950
Change on day -0.08%
Latest
US equities
Wall Street struggled for traction as concerns about the potential collapse of commercial lender CIT Group
FTSE 100 index
4600
4400
Change on day +0.35%
UK equities
Gains for banking stocks helped leave the FTSE 100 index on track for its best week since March after positive results from
950
900
850

刊登广告

比特币里的安全时间戳

- 直接把钱打到数据的Hash上，而不是一个公钥地址上
- 容易、兼容
- 消耗币、需要矿工一直追踪

- 使用OP_RETUTN,
- 返回错误代码、不能二次使用
- 便宜
- 非标准交易

OP_RETURN
<arbitrary data>

非法内容

没有办法防止

可以提高代价
P2SH

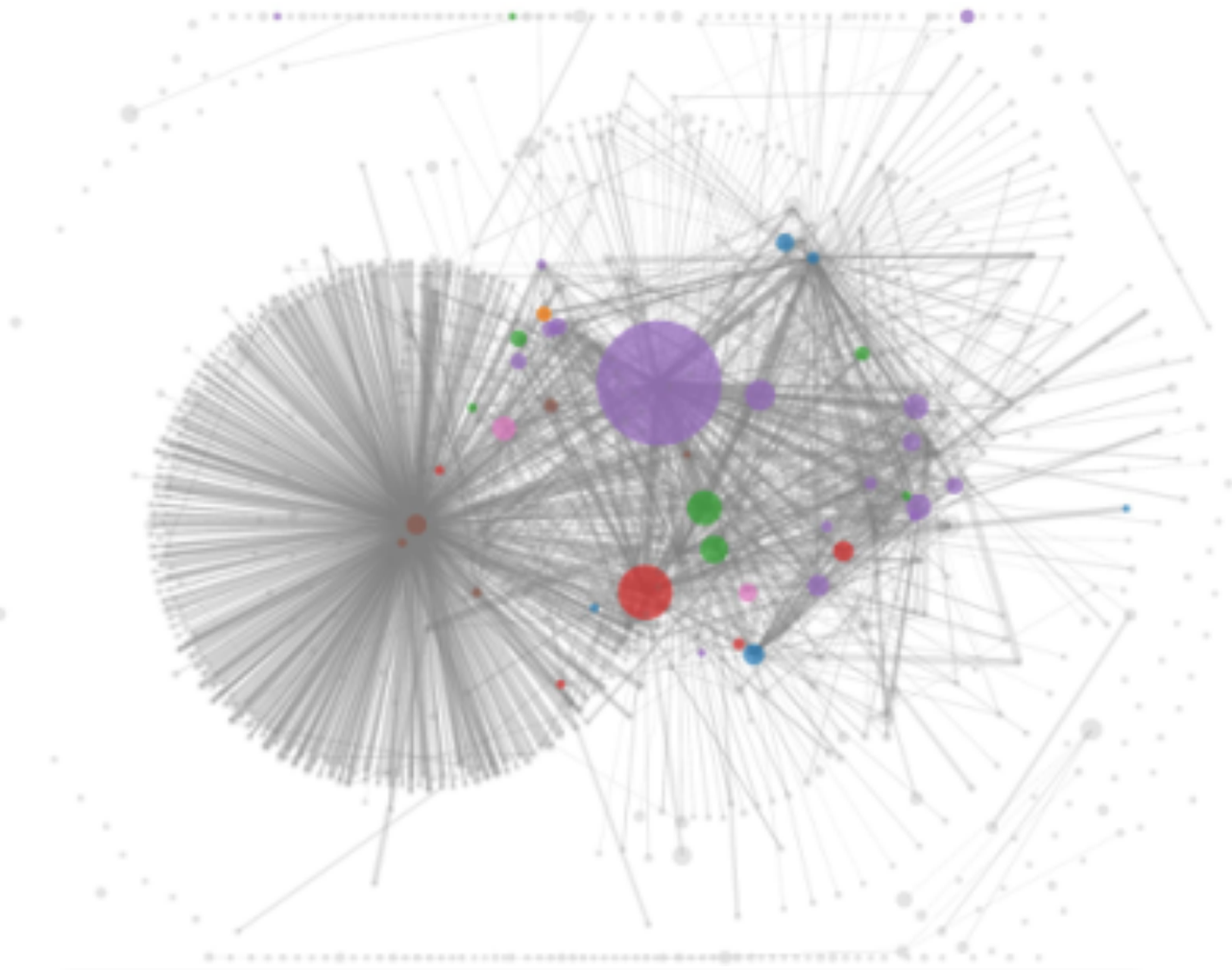
技术归技术

管理归管理

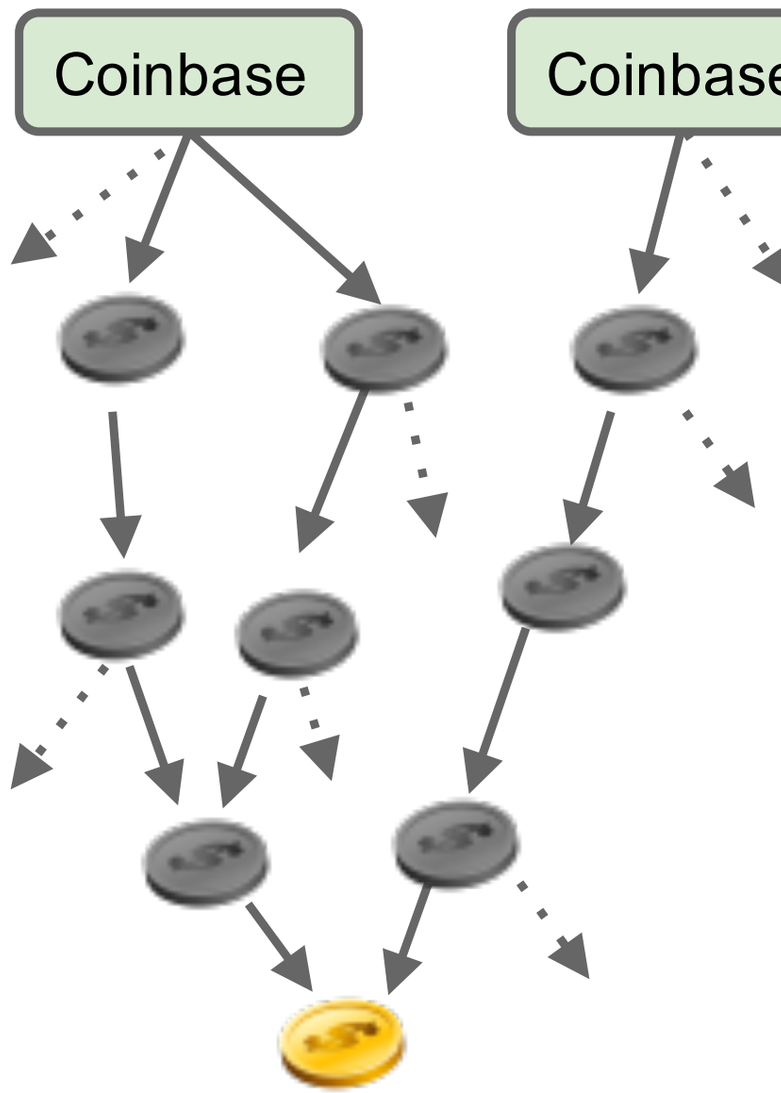
法律归法律

比特币交易历史

每一个比特币都是唯一的



每一个比特币都携带一些交易历史



可互换性

给货币增加元数据信息

成功平台的额外应用

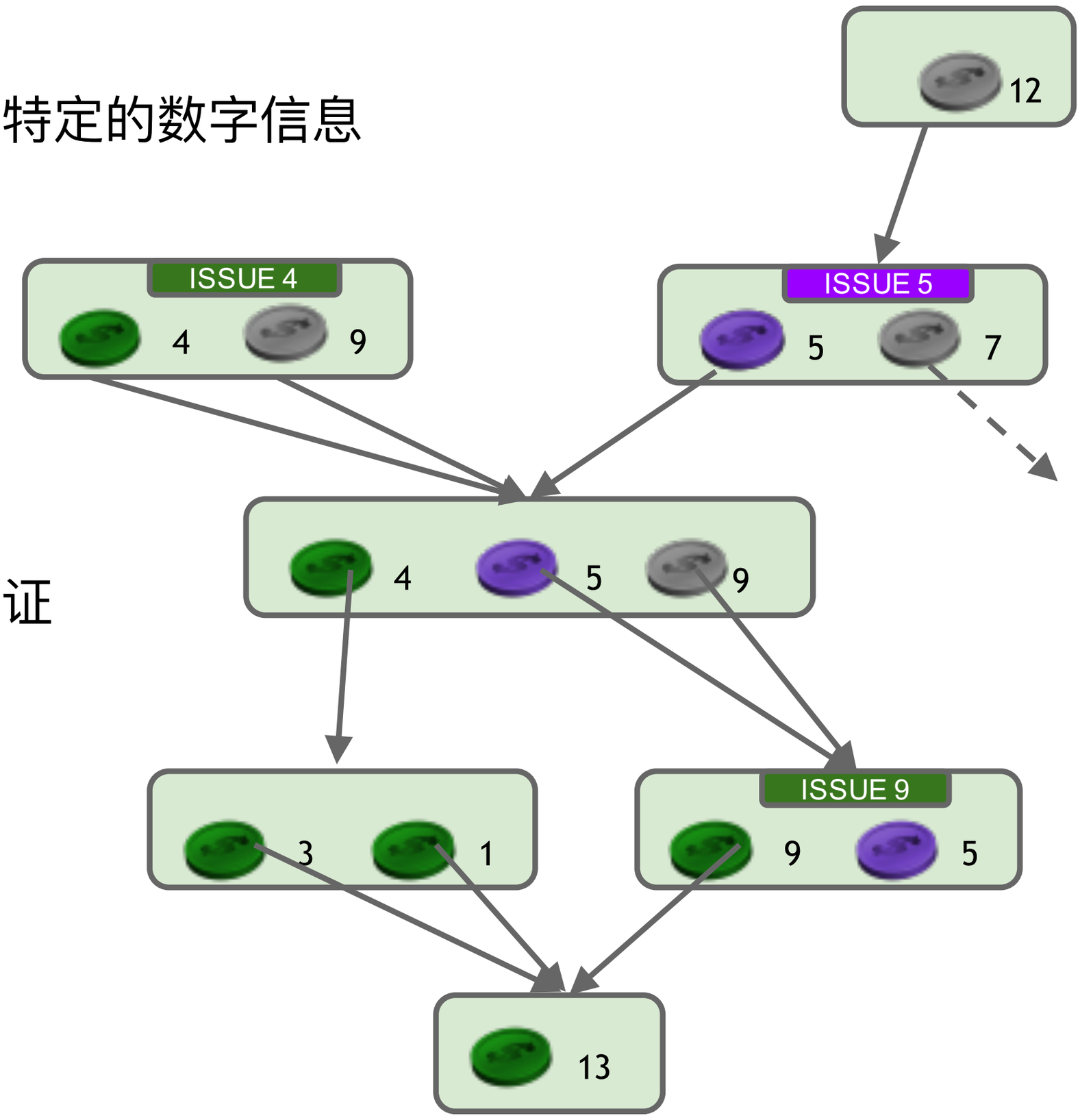
认证应用

"Bill #L11180916G hereby grants the holder admission to the Yankees game on Aug 18, 2014"

$SIGN_K(M, \#)$ →

染色币

染色：特定的数字信息



自己验证

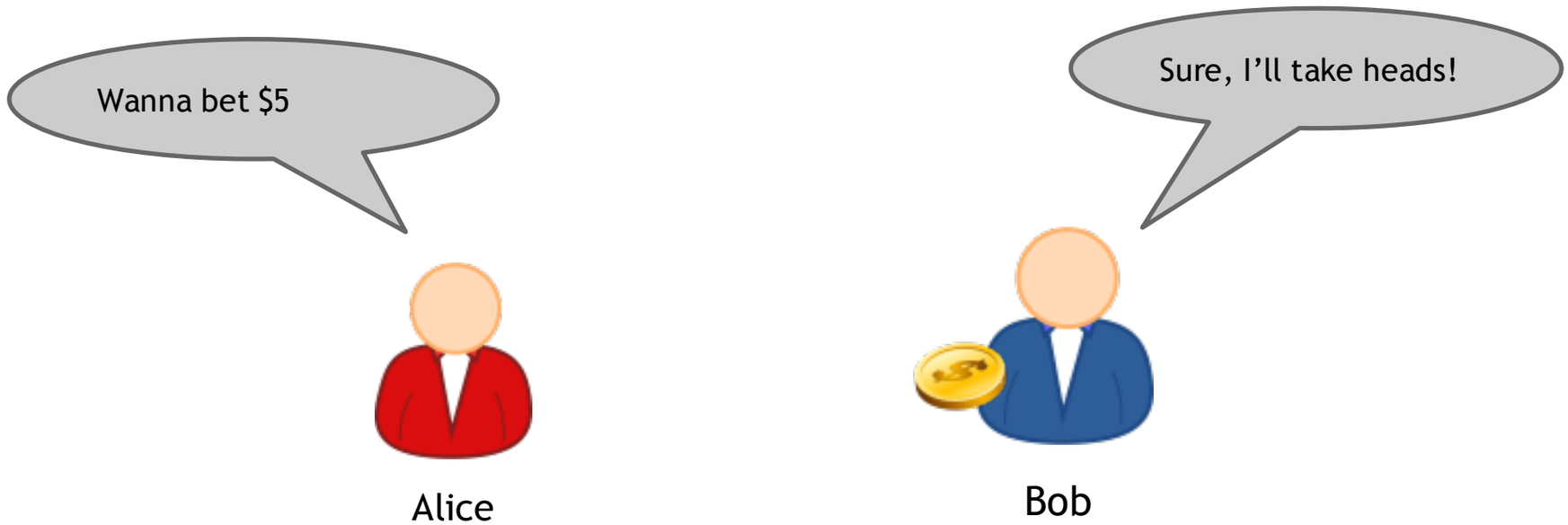
数字资产

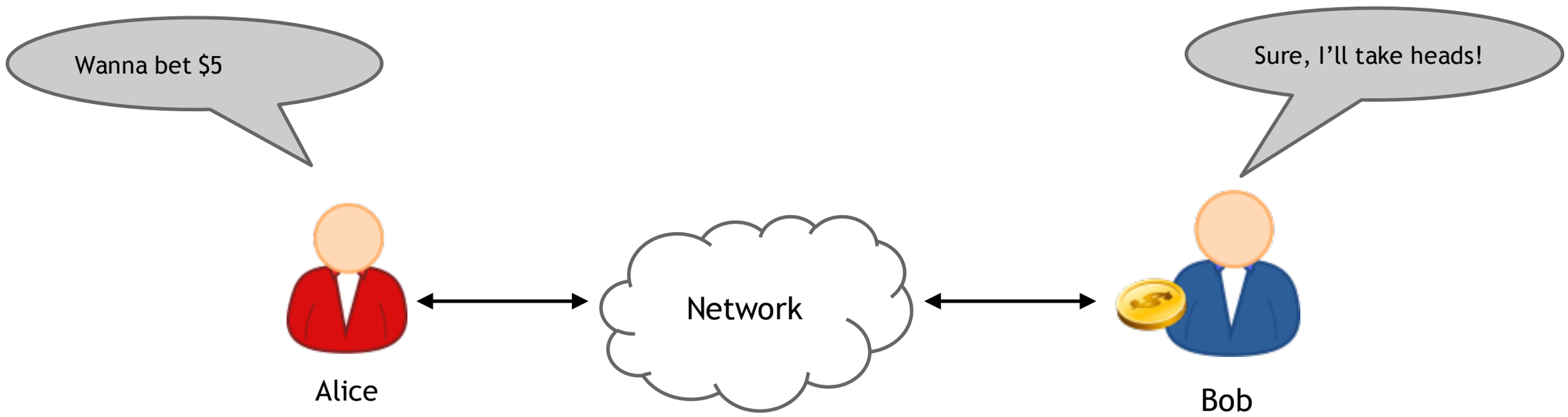
物理资产

股票

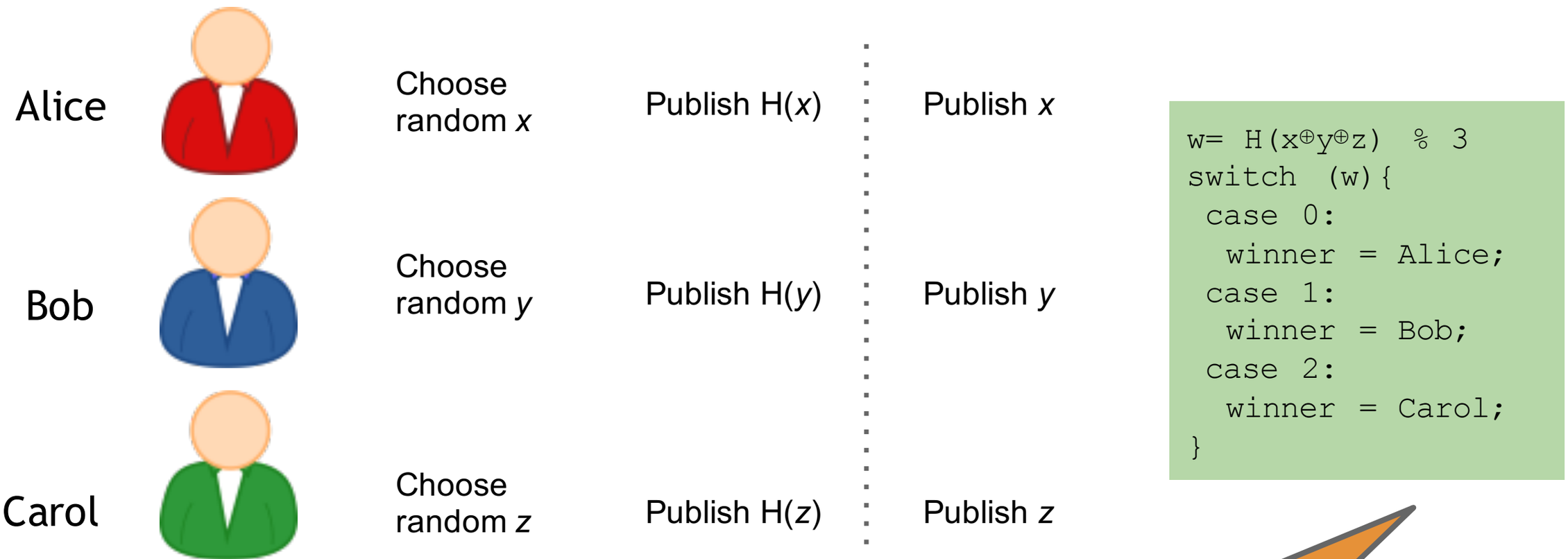
域名币

博彩

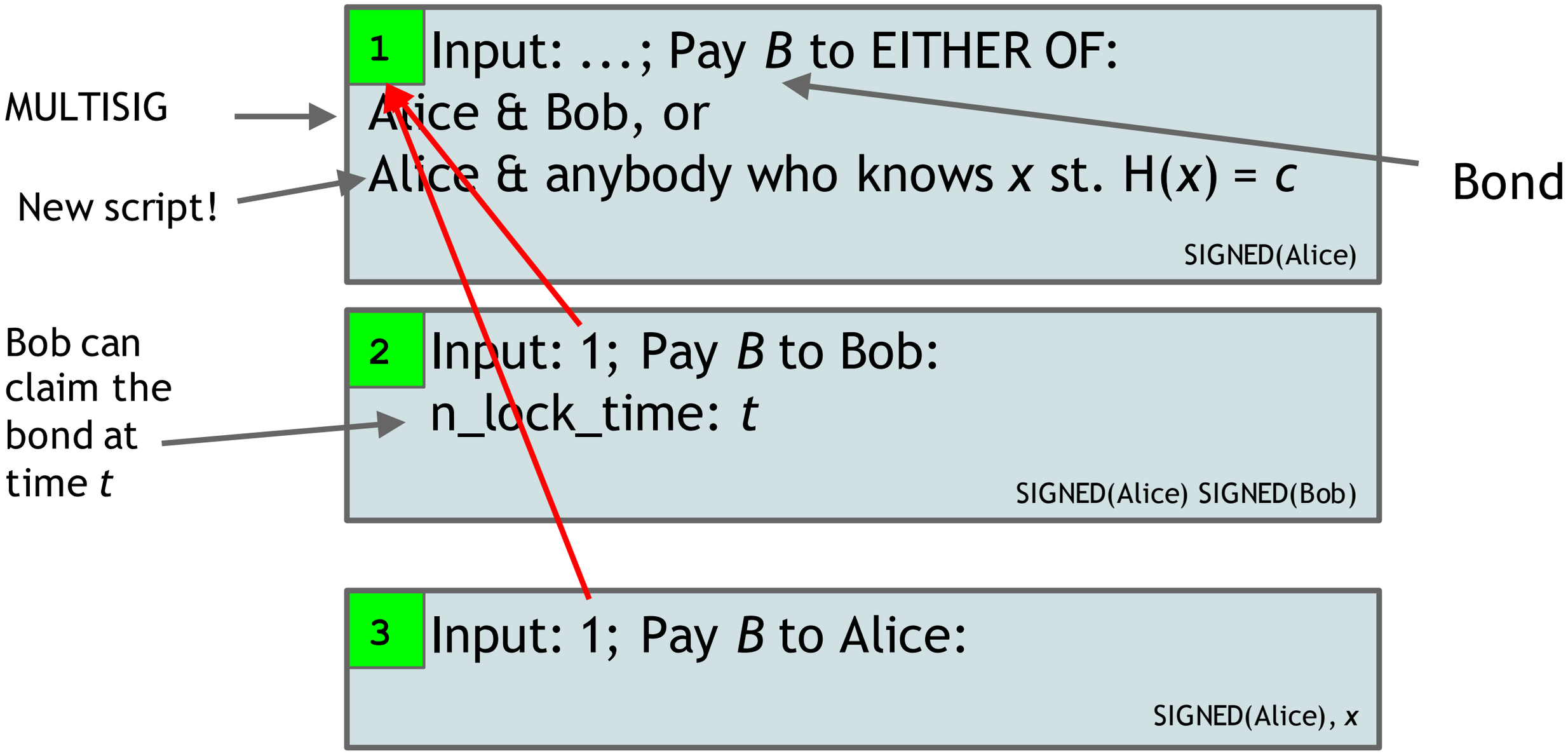

Wanna bet $5
Alice
Sure, I'll take heads!
Bob


Wanna bet $5
Alice
Network
Sure, I'll take heads!
Bob

在线博彩

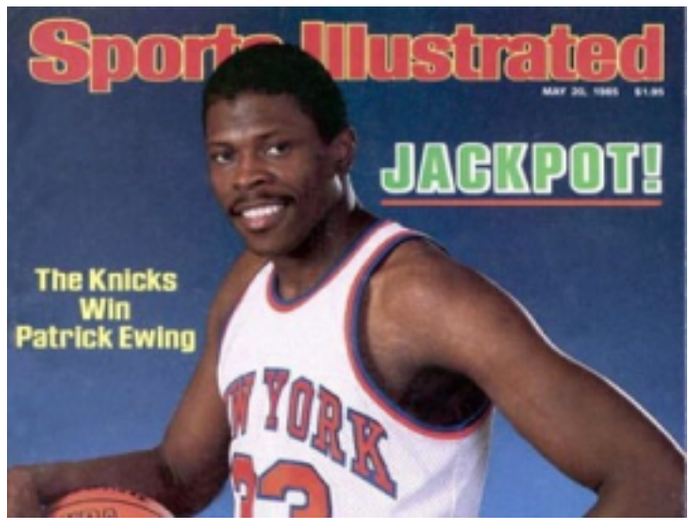

Round 1
Round 2
time
Alice
Choose random x
Publish H(x)
Publish x
Bob
Choose random y
Publish H(y)
Publish y
Carol
Choose random z
Publish H(z)
Publish z
w= H(x⊕y⊕z) % 3
switch (w){
case 0:
winner = Alice;
case 1:
winner = Bob;
case 2:
winner = Carol;
}
Hash function guarantees nobody can win with probability more than 1/3

时间约束的在线博彩

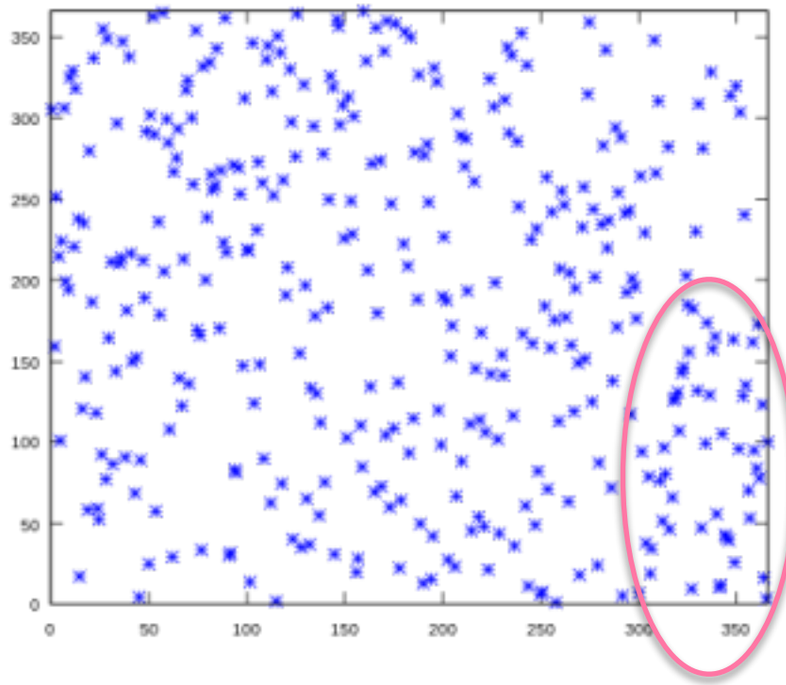

1
Input: ...; Pay B to EITHER OF:
Alice & Bob, or
Alice & anybody who knows x st. H(x) = c
SIGNED(Alice)
MULTISIG
New script!
Bond
2
Input: 1; Pay B to Bob:
n_lock_time: t
SIGNED(Alice) SIGNED(Bob)
Bob can claim the bond at time t
3
Input: 1; Pay B to Alice:
SIGNED(Alice), x
x revealed if Alice reclaims her bond

随机源

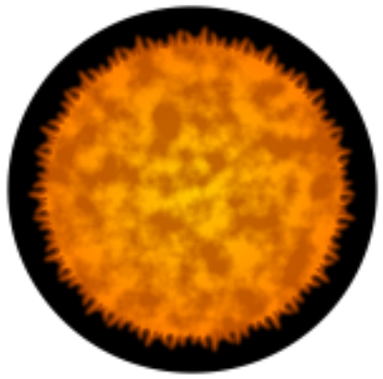

NBA
DRAFT
LOTTERY

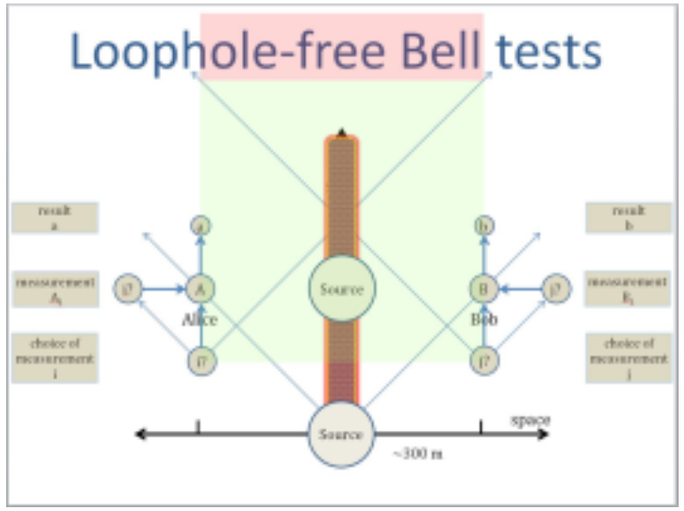

Sports Illustrated
JACKPOT!
The Knicks
Win
Patrick Ewing

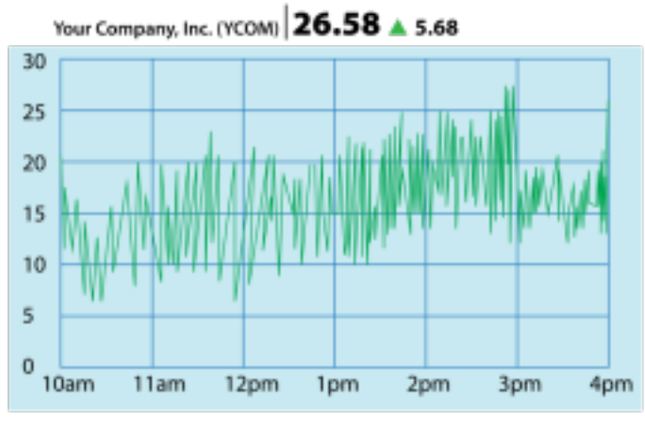

Bent Corner


350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
350

随机源

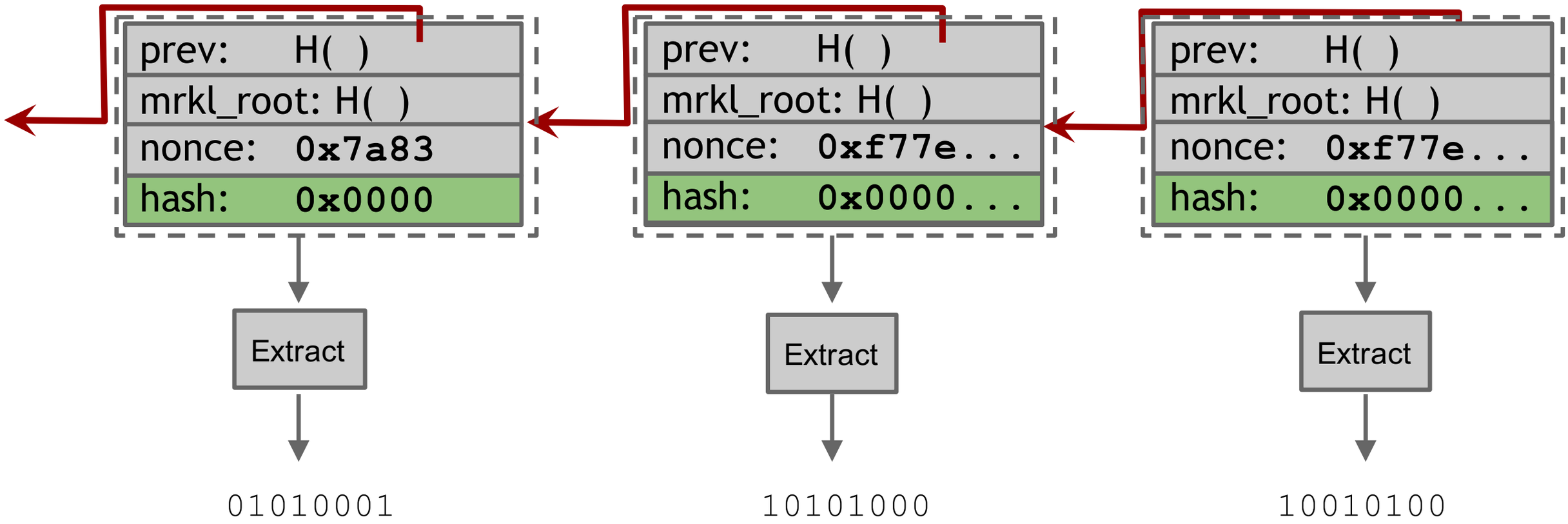



Loophole-free Bell tests
Source
Alice
Bob
Source
space
~300 m


Your Company, Inc. (YCOM) 26.58 ▲ 5.68
30
25
20
15
10
5
0
10am
11am
12pm
1pm
2pm
3pm
4pm


BINGO

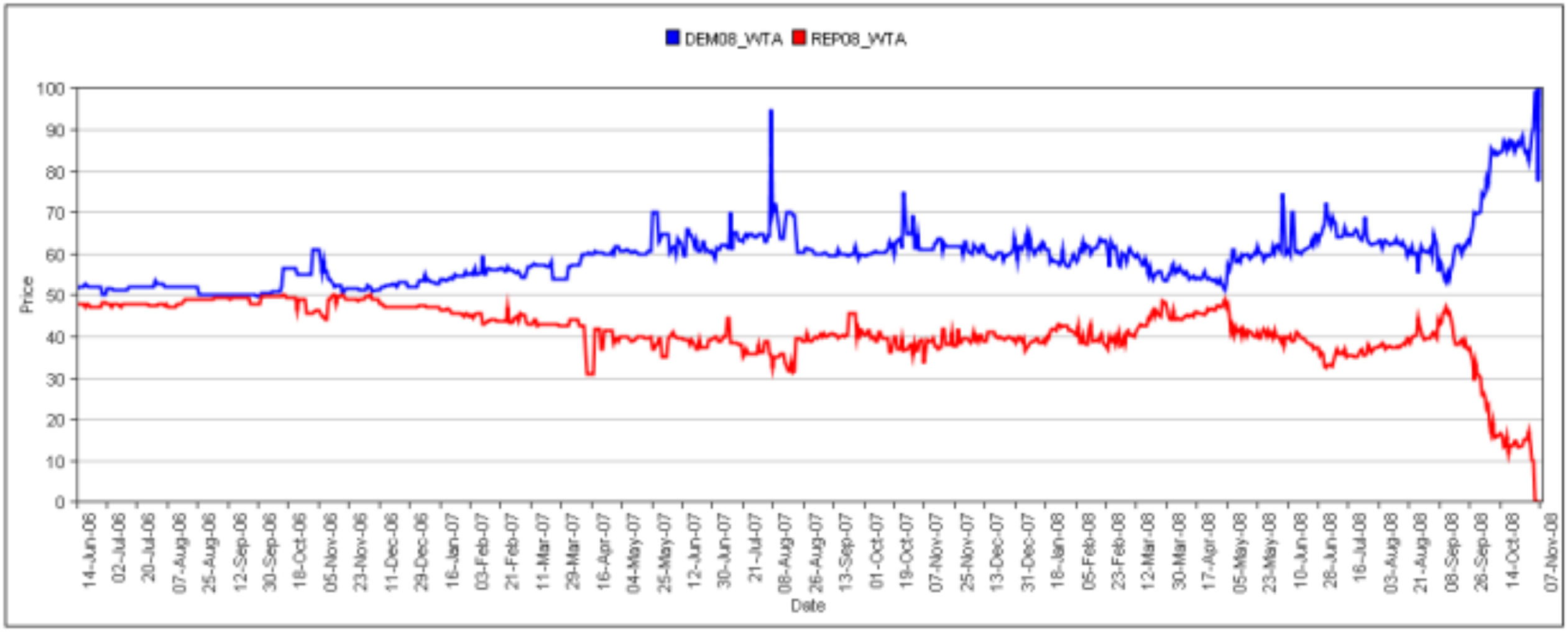
比特币作为随机源


prev: H( )
mrkl_root: H( )
nonce: 0x7a83
hash: 0x0000
Extract
01010001
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
Extract
10101000
prev: H( )
mrkl_root: H( )
nonce: 0xf77e...
hash: 0x0000...
Extract
10010100

预测市场

2014世界杯					
pre-tournament	0.12	0.09	0.22	0.01	0.05
after group stage	0.18	0.15	0.31	0.06	0.00
before semis	0.26	0.21	0.45	0.00	0.00
before finals	0.64	0.36	0.00	0.00	0.00
final	1	0	0	0	0

2008总统选举



Iowa Electronic Markets

Blockchain Application

Reality Keys

REALITY KEYS Pricing Developers Legal Privacy About

Facts about the future, cryptographic proof when they come true.

39 million topics

Follow a Freebase fact

Will Hillary Clinton become US President?

Will Edward Snowden win a Nobel Peace Prize?

You can follow facts about any of the 39 million topics in the Freebase open directory.

Exchange rates

Follow an exchange rate

Will a Dollar be worth more than a Euro?

Will Bitcoin hit $1000 again?

We track the exchange rates of traditional currencies and crypto-currencies.

Blockchain addresses

Follow a transaction

I'm selling Litecoins for Bitcoins. Have I been paid?

Are the bitcoins seized from Silk Road still there?

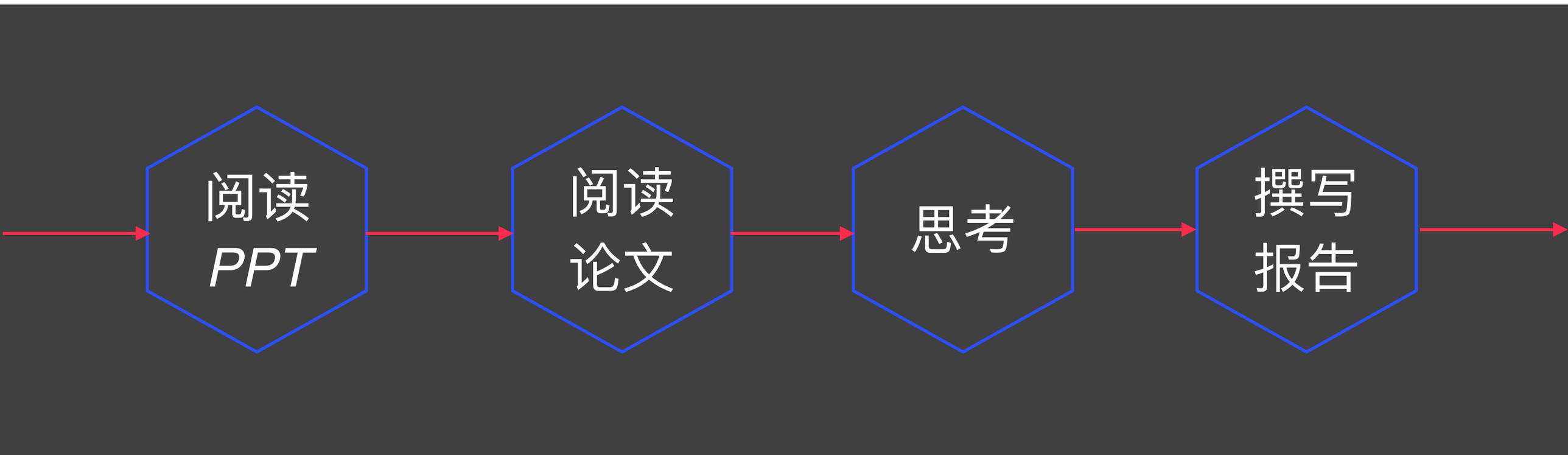
You can follow any transaction in the blockchain of Bitcoin or any crypto-currency we monitor.

优缺点

Orange?

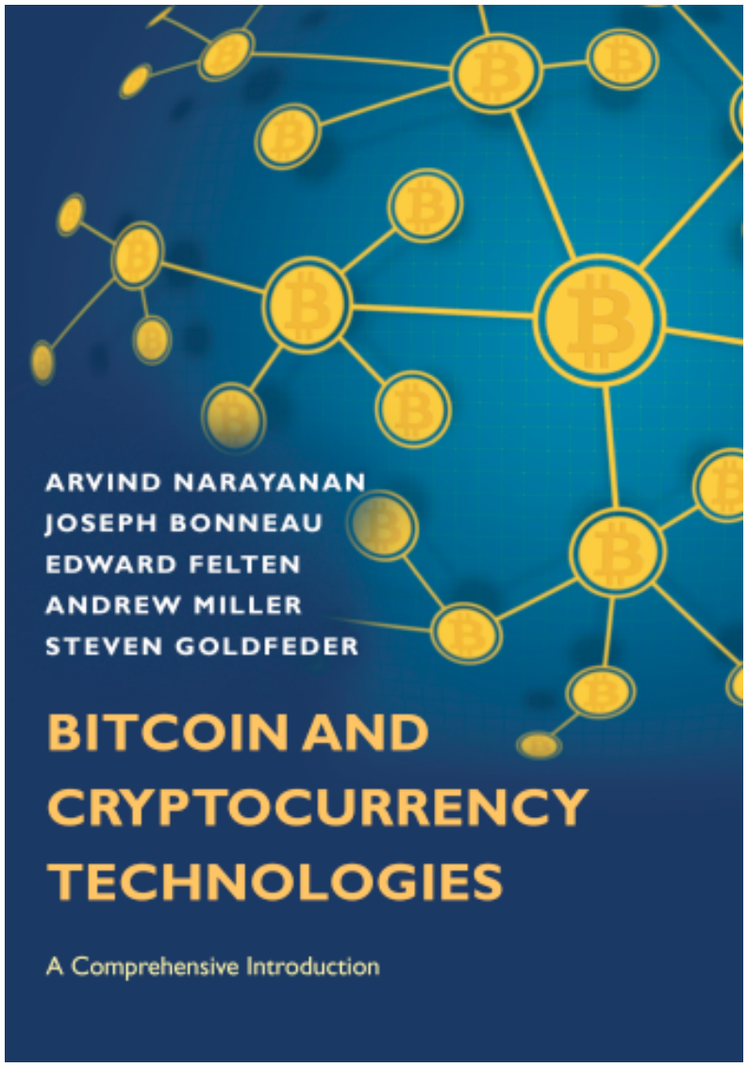
Yellow?

课后作业



Homework

阅读教材



阅读第9章

Homework

课后作业

要求阅读如下文章，写阅读报告

In IEEE Software Magazine 2020

Blockchain Technologies in Practice

Christof Ebert, Panos Louridas, Tiago M. Fernández-Caramés, and Paula Fraga-Lamas

https://ieeexplore.ieee.org/document/9121627

检索一篇区块链应用的好文章
如果和保险和车应用更好

1、文章概述
2、主要收获
3、存在疑问
4、所思所感
5、一篇论文

周日晚上12点前提交

Homework

课程项目

- 选择一个身份认证或区块链相关的内容
  - ✳ 总计分析该方向的研究现状，完成开题报告
  - ✳ 完成一个算法、机制、系统、方案

- 具体要求

>>>> 阅读最新的顶会的文章并延续 <<<<

  - ✳ 每组4人以内，自由组队；本周发到群里，12月15日前确定选题
  - ✳ 方向越小越好：口令、验活、区块链隐私、分片、共识等
  - ✳ 检索：知网、google学术、google等
  - ✳ 12月20日完成开题报告，1月10日提交最终报告+ppt，1月13日报告

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io