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

课堂测试时间

课堂测试02

20－30分钟

- 1、什么是UTXO，简单介绍其结构和作用。
- 2、简单描述比特币中有哪些地方用到了密码学的哪些机制
- 3、简单描述比特币是如何挖矿的，为什么要动态调整挖矿难度，是如何调整的。
- 4、钱包有哪几类，简单描述每类的优缺点。
- 5、P2SH的含义是什么，为什么需要使用P2SH，简单描述使用流程。
- 6、读完这篇文档，你有新的感想、想法和问题。

上次课程内容

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

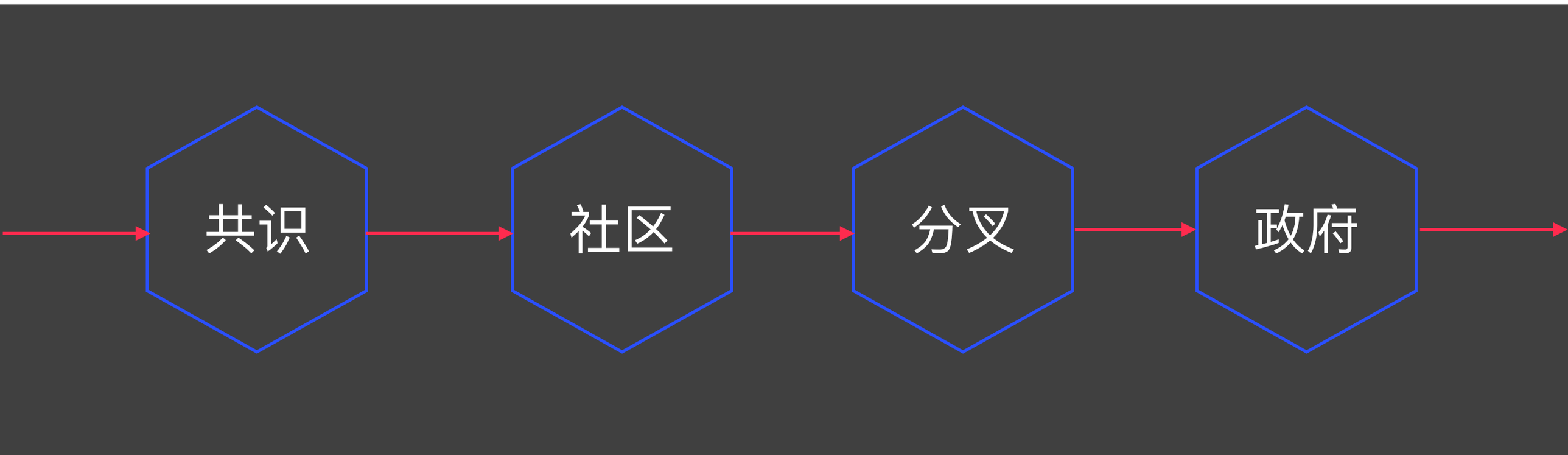
3 匿名

- 隐私
- 匿名
- 如何实现
- 混币

4 剖析

- 矿池
- 挖矿扩展
- 性能
- 性能扩展

监管



关于比特币的共识

机制

关于规则的共识

关于比特币价值的共识

关于历史纪录的共识

账本

仙子效应

谁掌握比特币

MIT许可协议

比特币改进方案BIP

核心钱包发人员

分叉

核心开发人员：规则和代码

矿工：验证交易、编写历史纪录

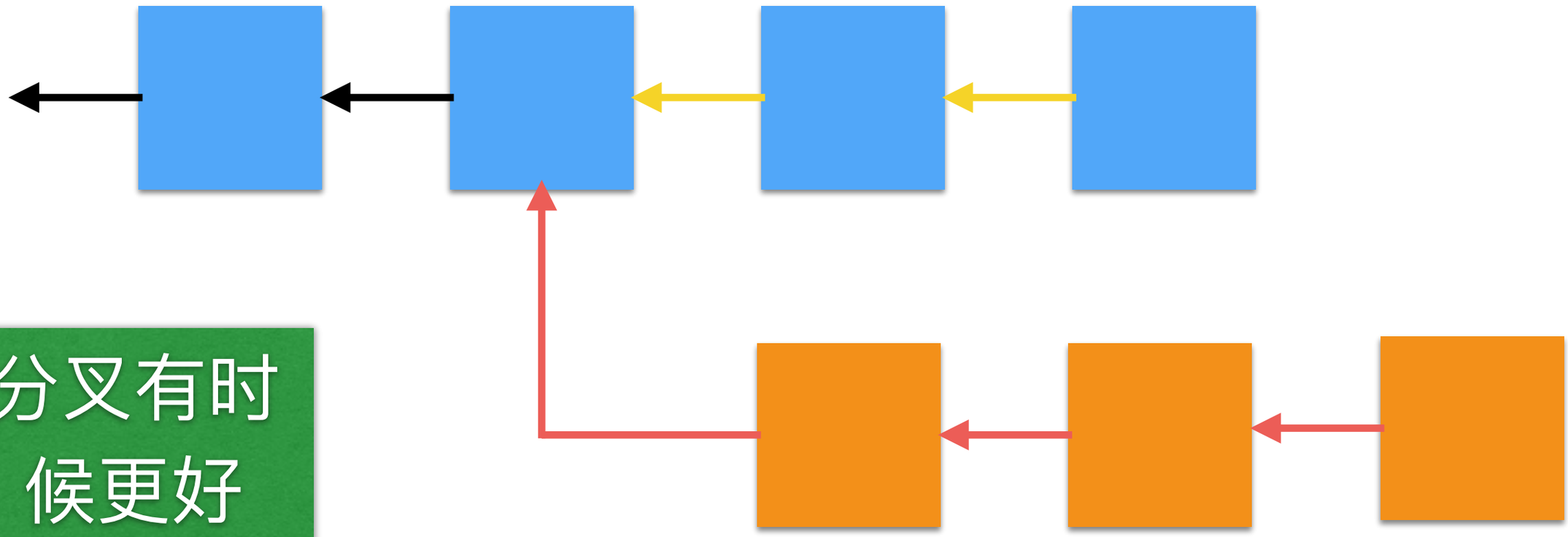
投资人：购买

商家：采用与否

支付服务商：法币兑换

基金会：宣传推广

比特币分叉



分叉有时候更好

块大小

1M

2M

4M

8M

不限制

SEGWIT

隔离见证

250/100

闪电网络

比特币分叉

香港共识

SegWit

BP141

BP148

纽约共识

SegWit2x

BP91

UASF

bitcoin

BITCOINGOLD

以太坊分叉

The DAO 攻击

政府态度

政府管控：禁止、严格管控、不严格

资本管制

犯罪

反洗钱

KYO

强制上报

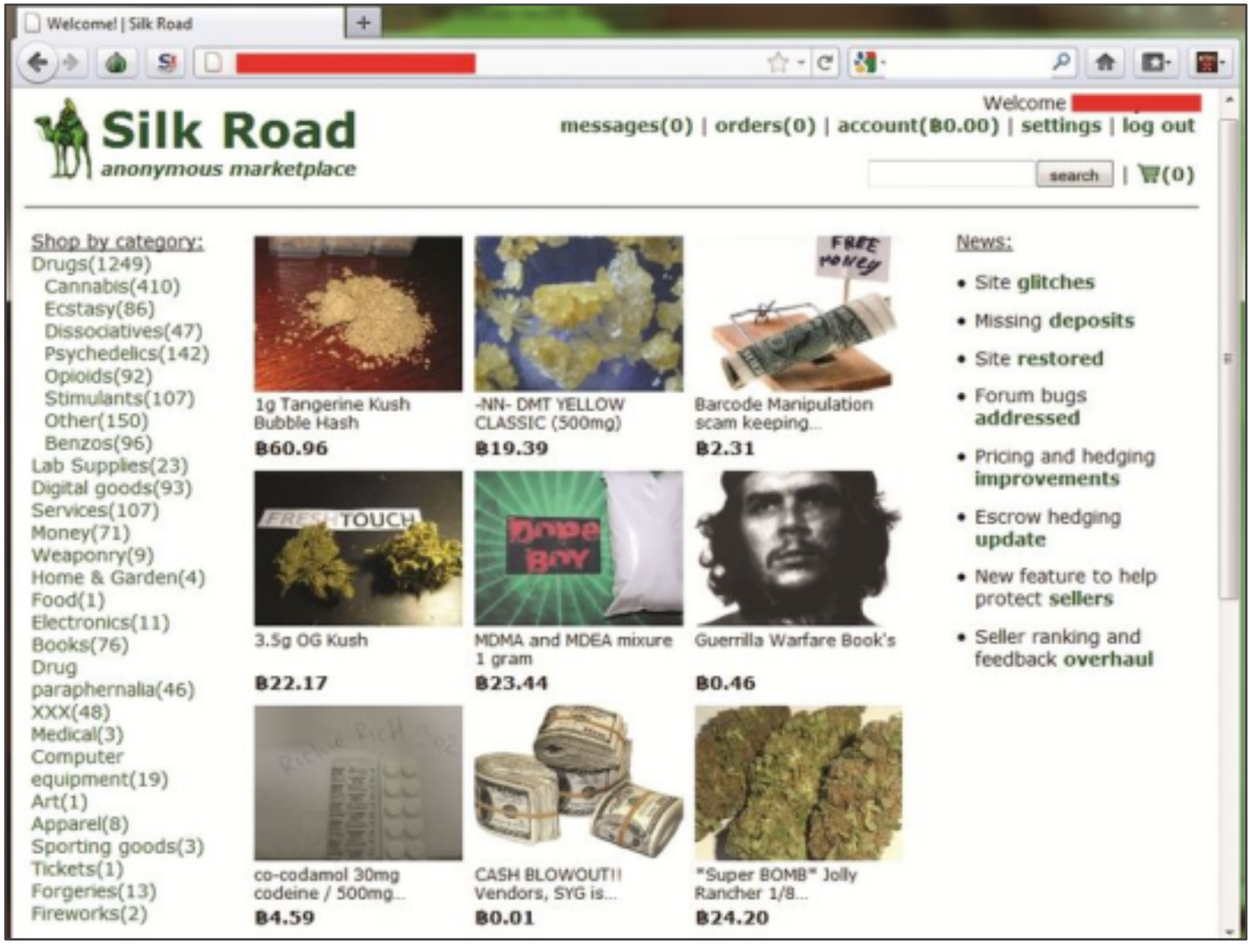
纽约州比特币牌照

美国加密货币管理政策

中国政府2017年系列政策

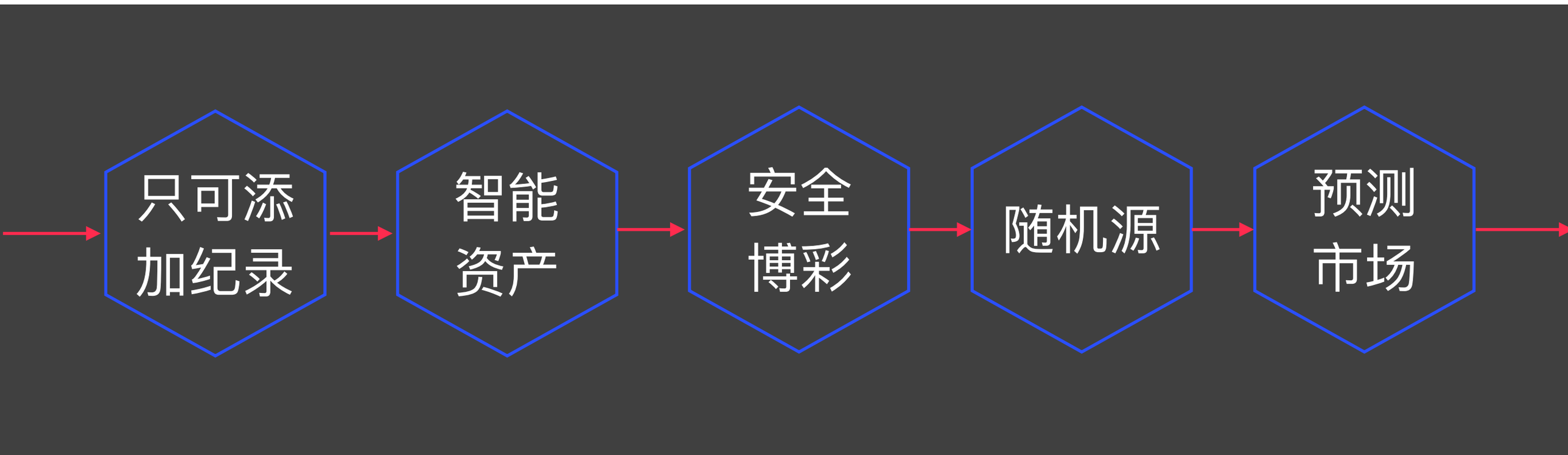
日韩新加坡

丝绸之路



把现实世界和虚拟世界完全分离开是很困难的

比特币作为平台



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

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-HHPAMP
VRUBSC-7DQE7O-TZBCP4-MS5S65
UBOSEC-UU2A3N-OCCCIR-PLM4PG
MARK
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
FTSE Eur
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、需要矿工一只追踪

- 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

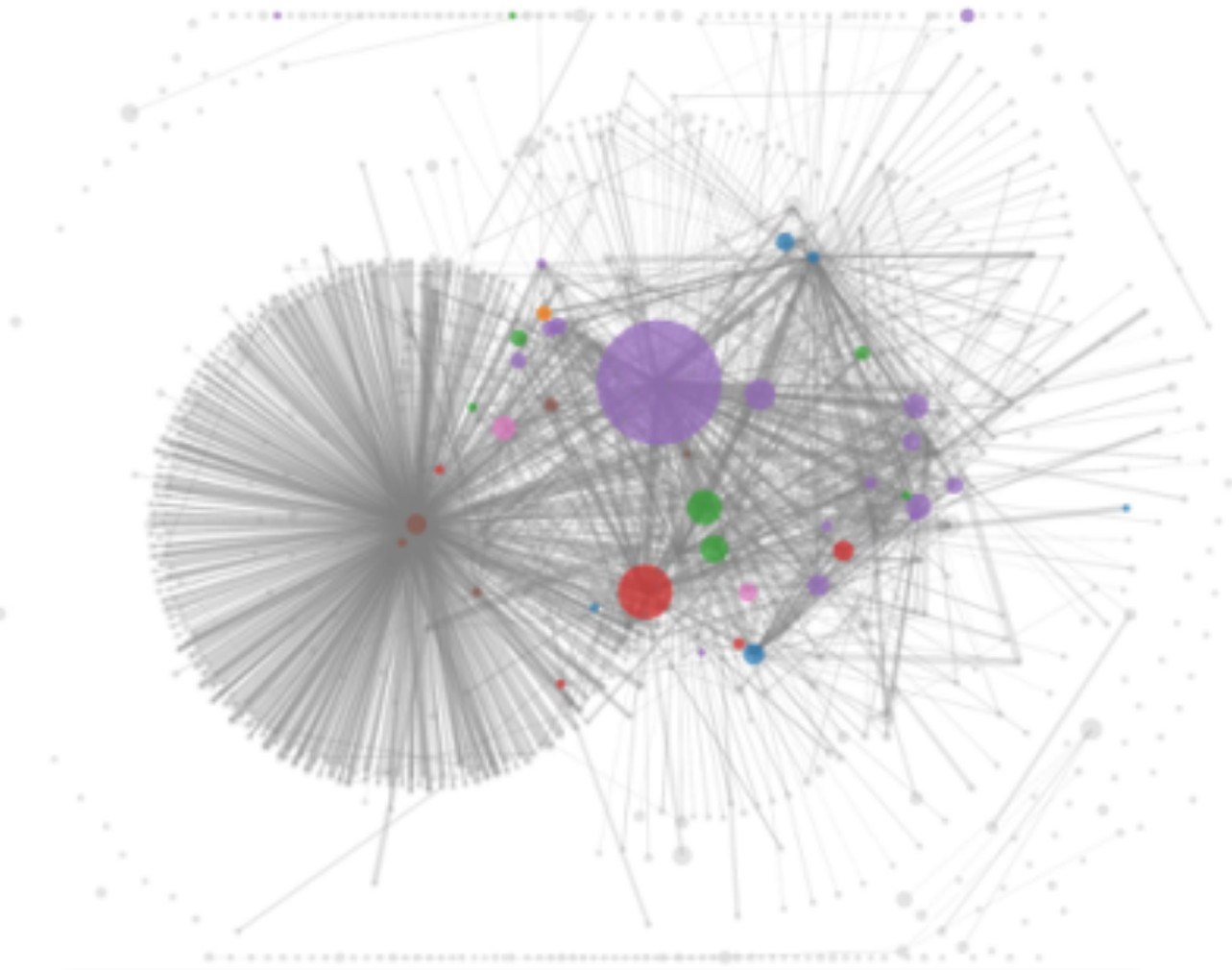
技术归技术

管理归管理

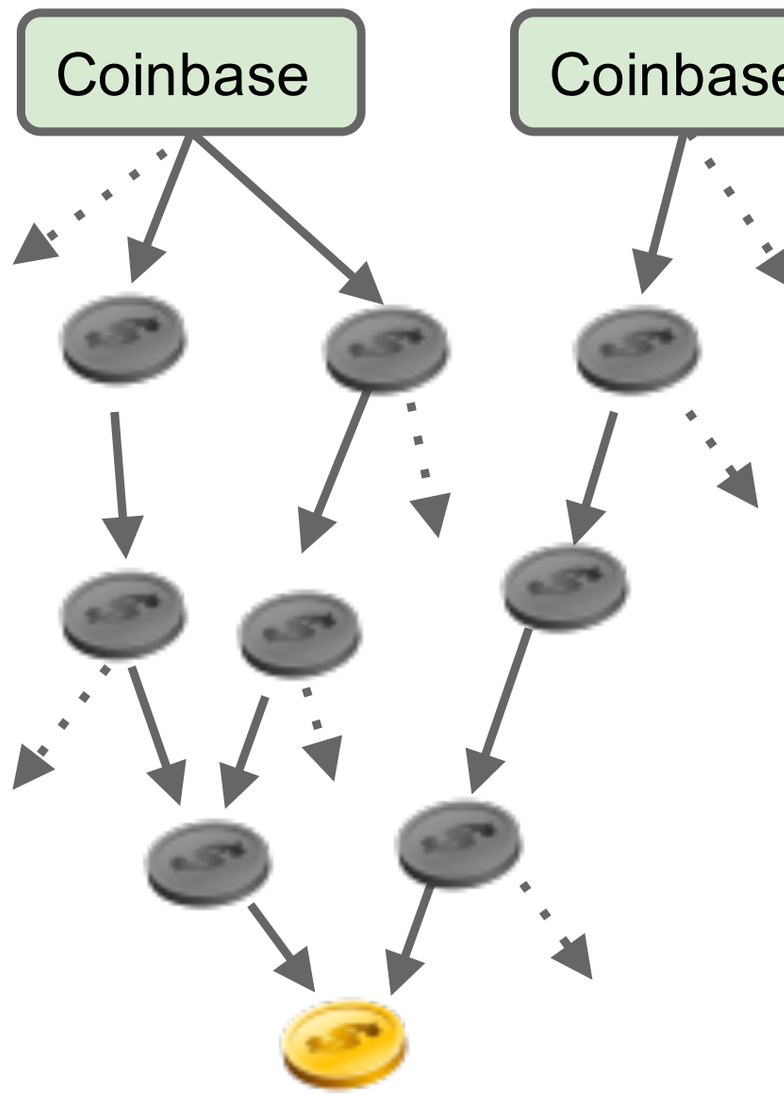
法律归法律

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

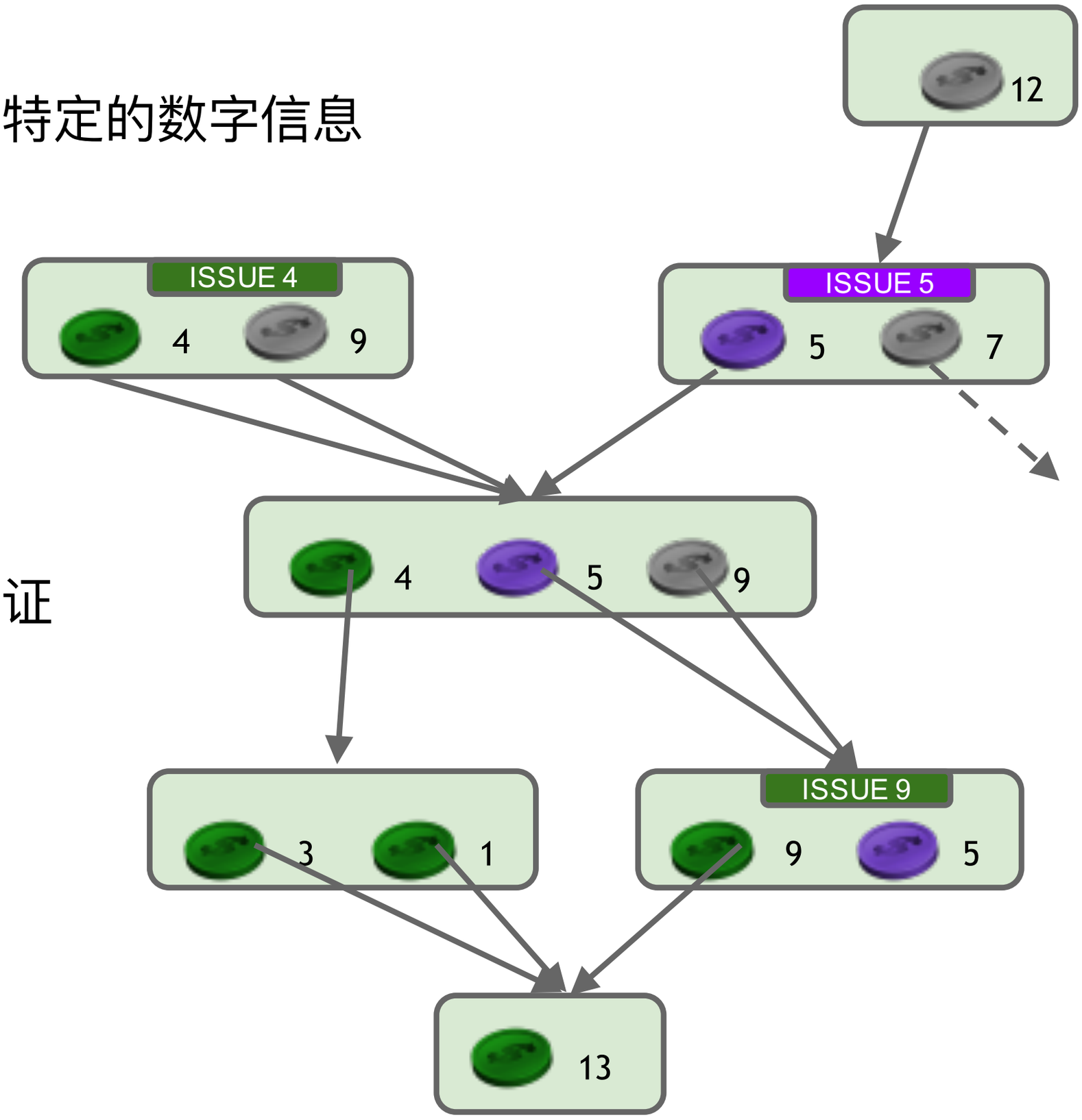
认证应用

"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

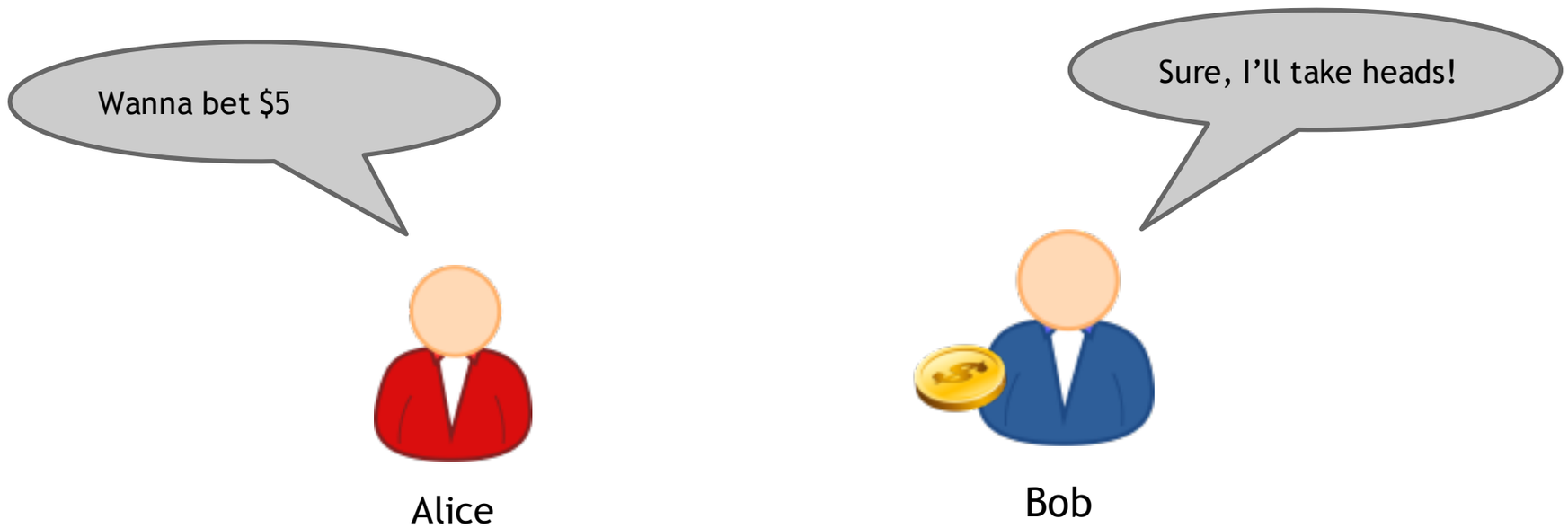
数字资产

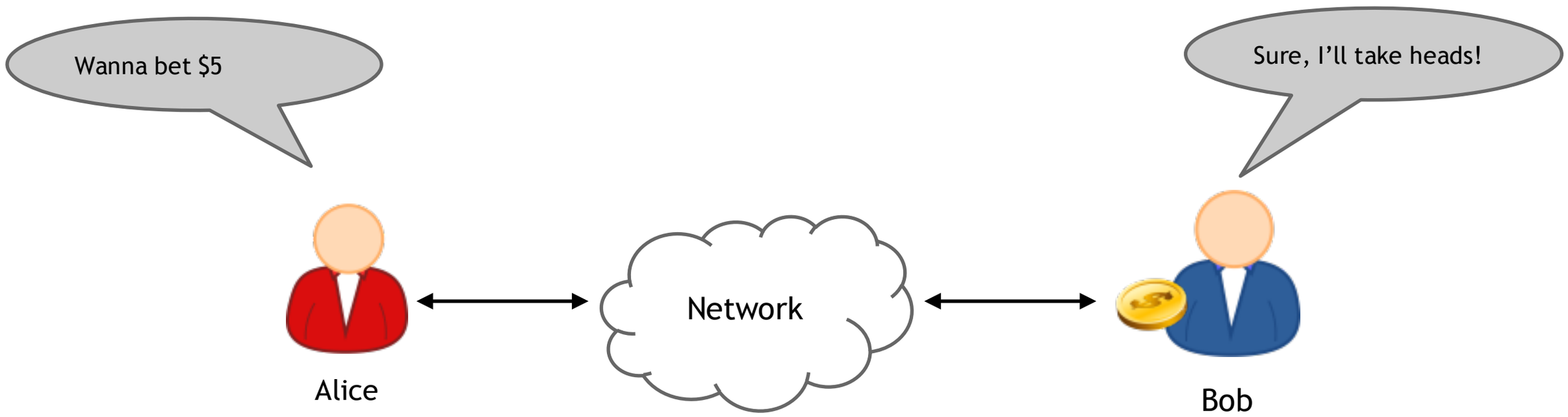
物理资产

股票

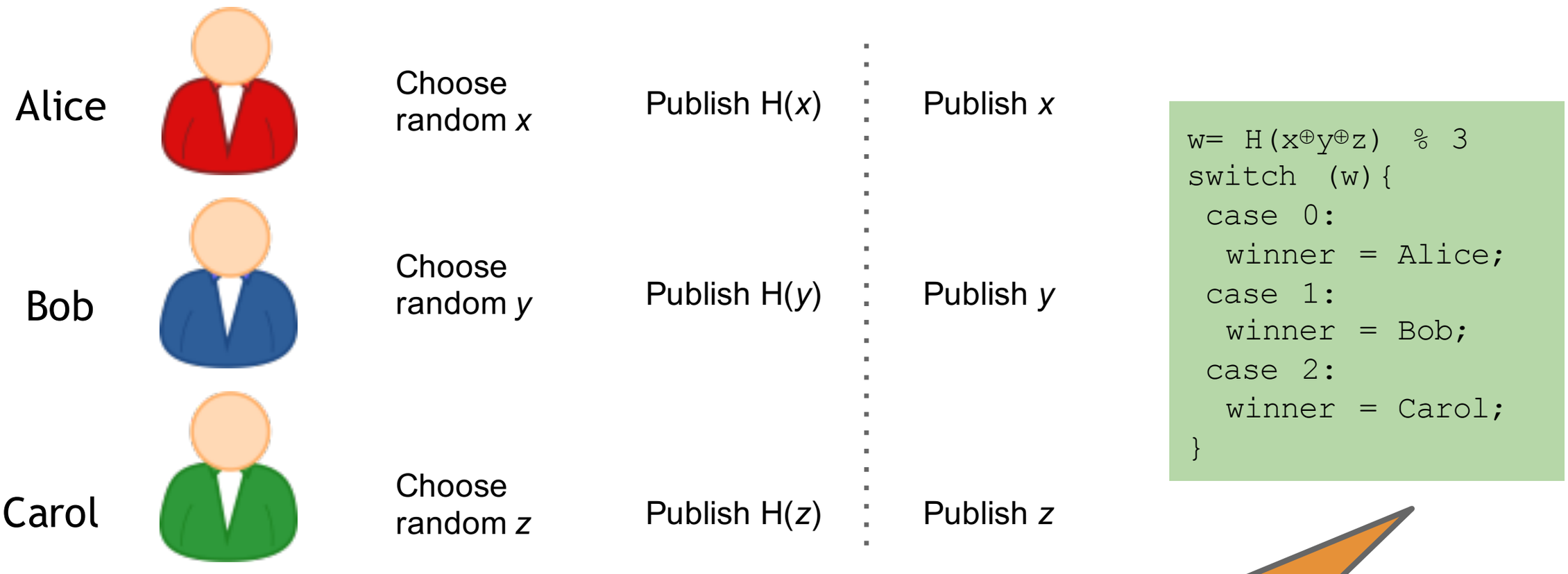
域名币

博彩

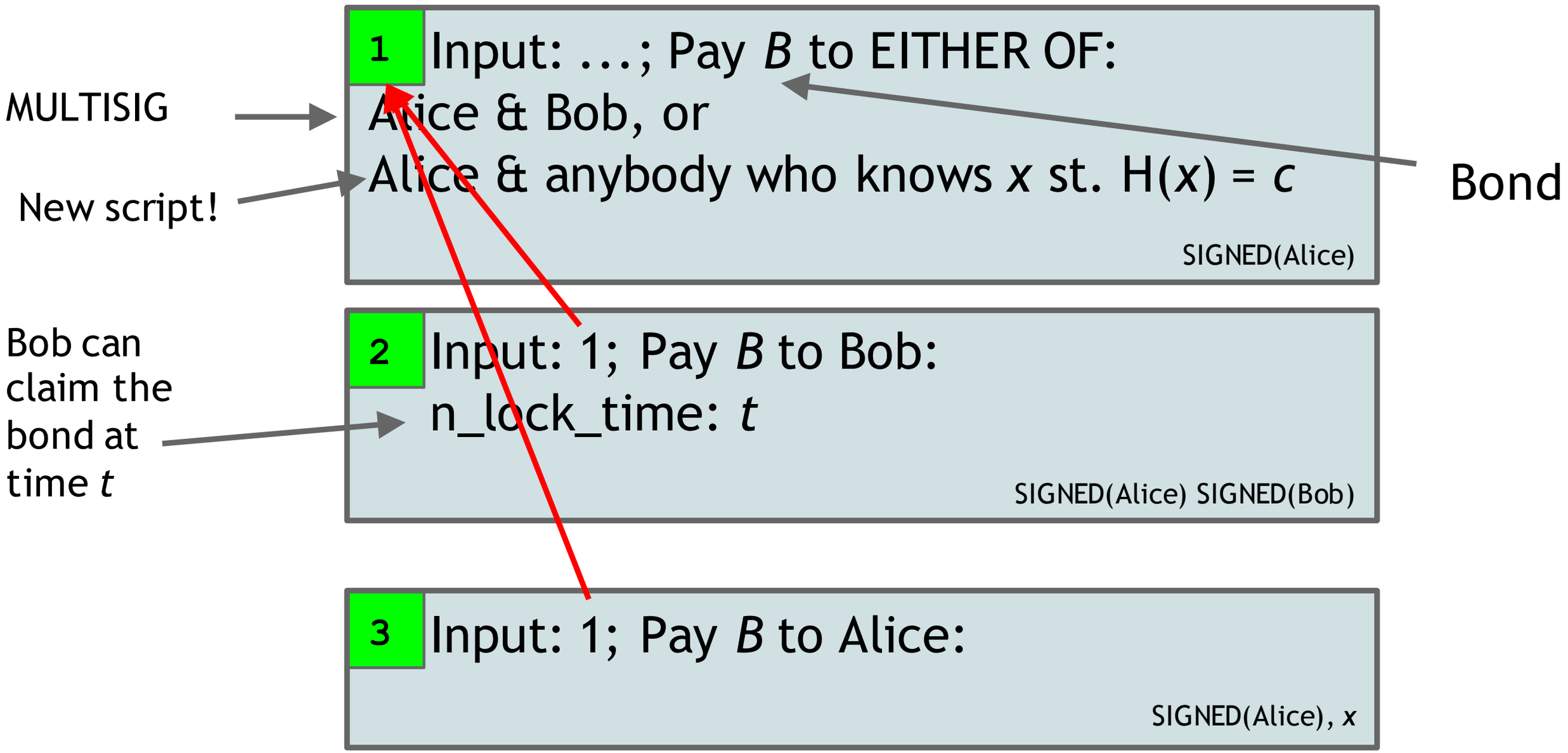

Wanna bet $5
Alice
Sure, I'll take heads!
Bob


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

在线博彩

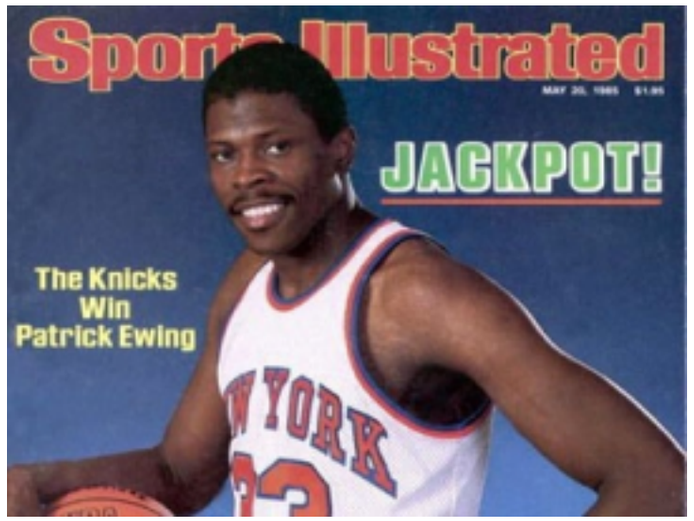

Round 1
Round 2
time
Alice
Choose random x
Publish H(x)
Publish x
Bob
Choose random y
Publish H(y)
Publish y
Carol
Choose random z
Publish H(z)
Publish z
w= H(x⊕y⊕z) % 3
switch (w){
case 0:
winner = Alice;
case 1:
winner = Bob;
case 2:
winner = Carol;
}
Hash function guarantees nobody can win with probability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

时间约束的在线博彩

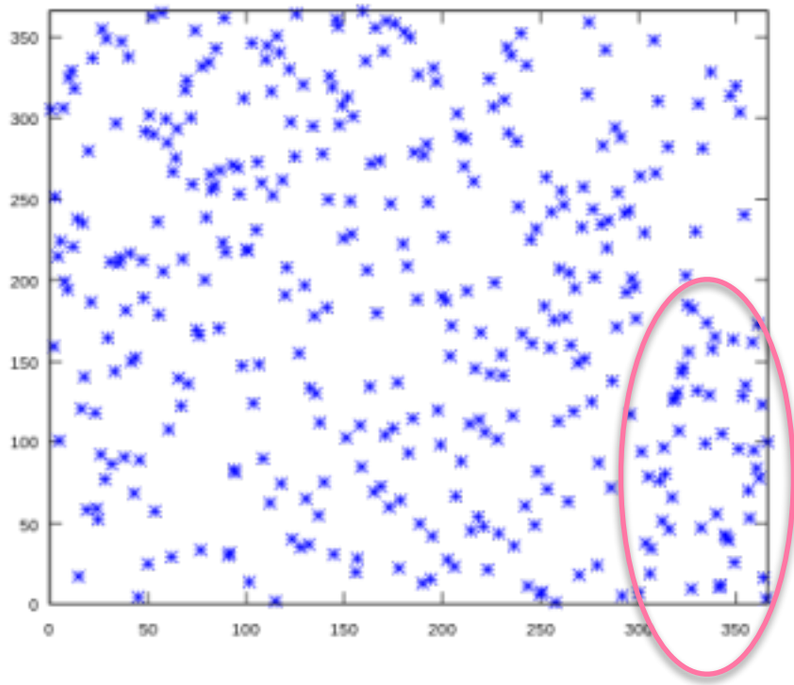

1
Input: ...; Pay *B* to EITHER OF:
Alice & Bob, or
Alice & anybody who knows *x* st. H(*x*) = *c*
SIGNED(Alice)
MULTISIG
New script!
Bond
2
Input: 1; Pay *B* to Bob:
n_lock_time: *t*
SIGNED(Alice) SIGNED(Bob)
Bob can claim the bond at time *t*
3
Input: 1; Pay *B* to Alice:
SIGNED(Alice), *x*
x revealed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

随机源

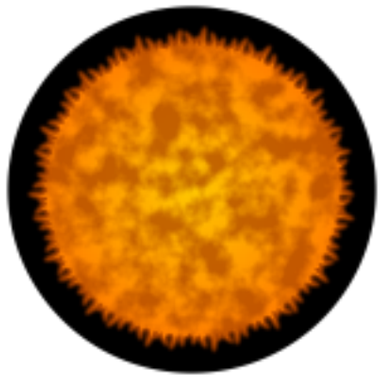

NBA
DRAFT
LOTTERY

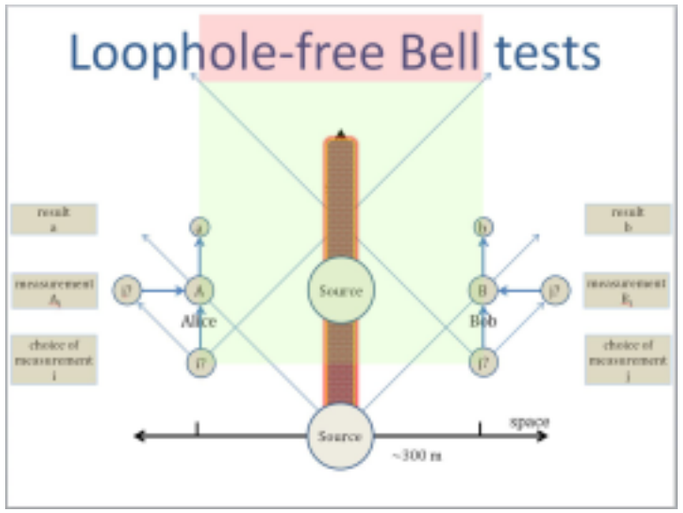

Sports Illustrated
JACKPOT!
The Knicks
Win
Patrick Ewing

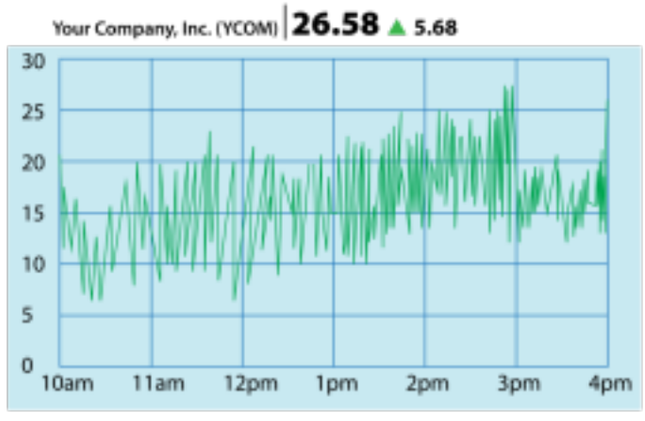

Bent Corner


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

随机源

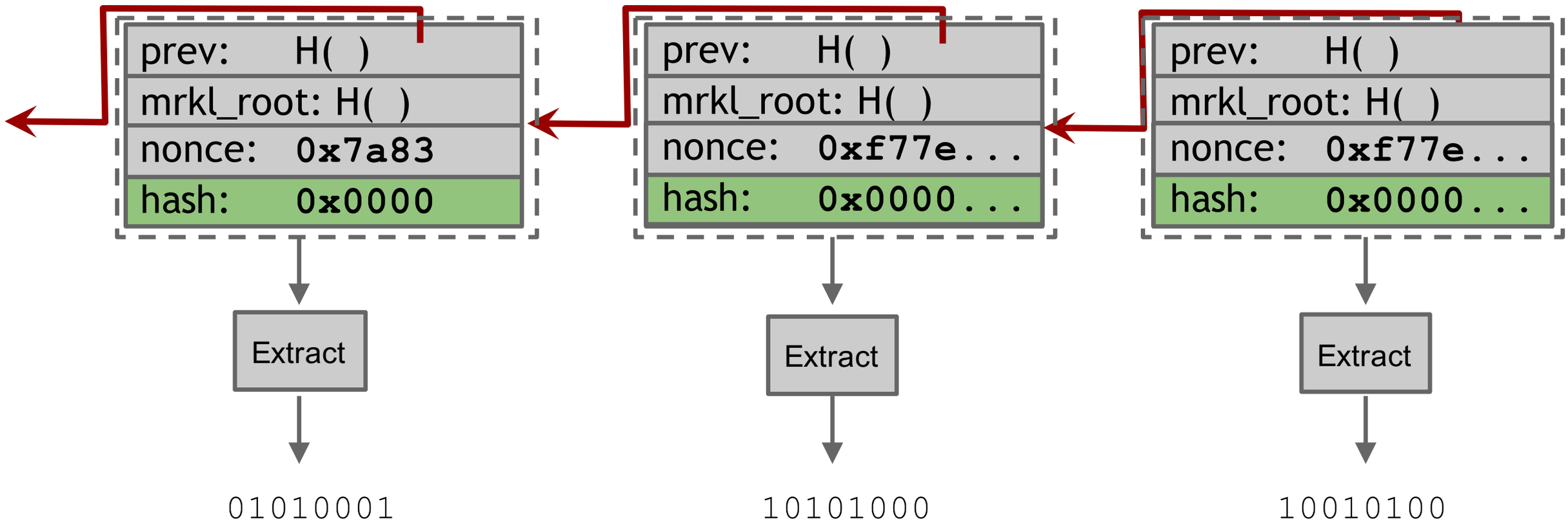



Loophole-free Bell tests
Source
Alice
Bob
Source
space
~300 m


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


BINGO

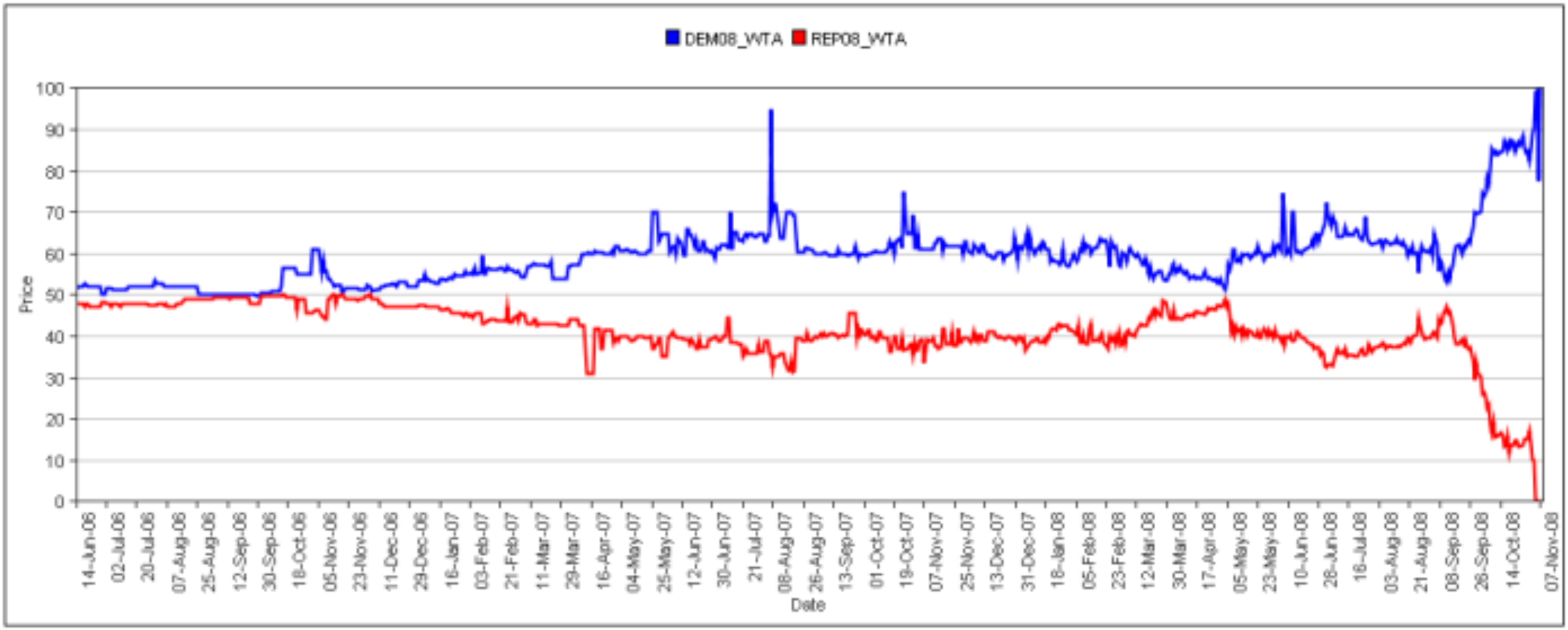
比特币作为随机源


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

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?

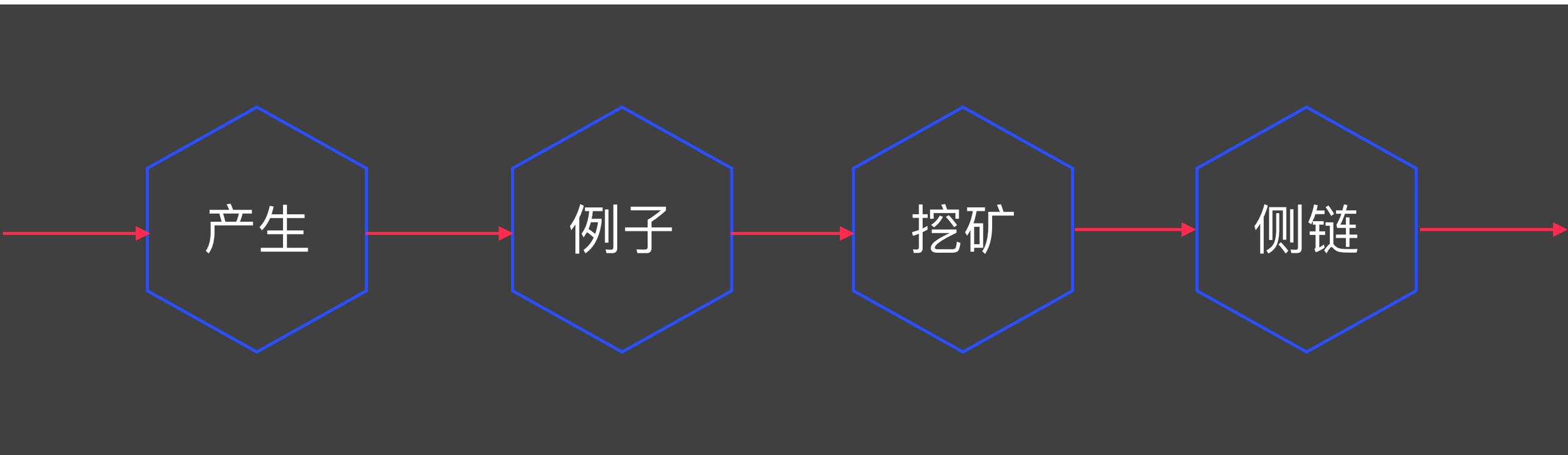
You can follow any transaction in the blockchain of Bitcoin or any crypto-currency we monitor.

优缺点

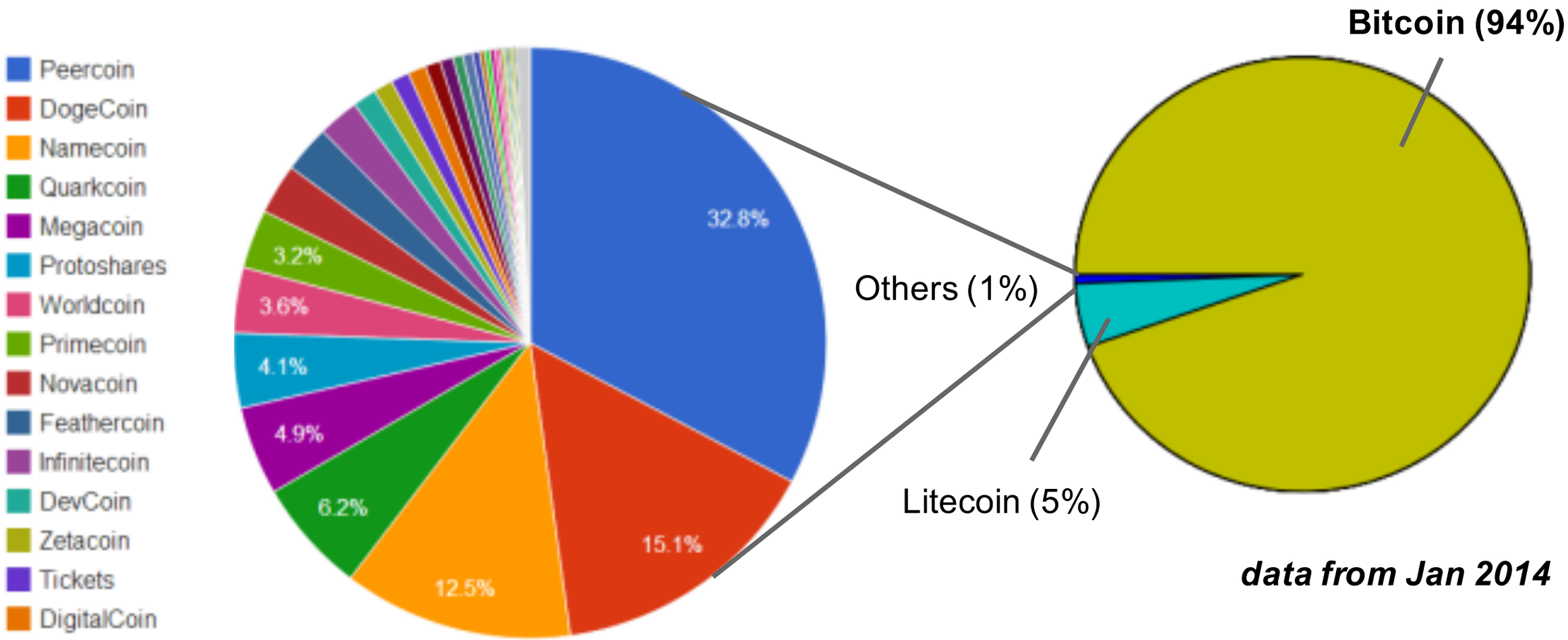
Orange?

Yellow?

其余代币



加密货币


Peercoin
DogeCoin
Namecoin
Quarkcoin
Megacoin
Protoshares
Worldcoin
Primecoin
Novacoin
Feathercoin
Infinitecoin
DevCoin
Zetacoin
Tickets
DigitalCoin
32.8%
15.1%
12.5%
6.2%
4.9%
4.1%
3.6%
3.2%
Others (1%)
Litecoin (5%)
Bitcoin (94%)
data from Jan 2014

一些代币

为什么发行

吸引矿工

如何发行

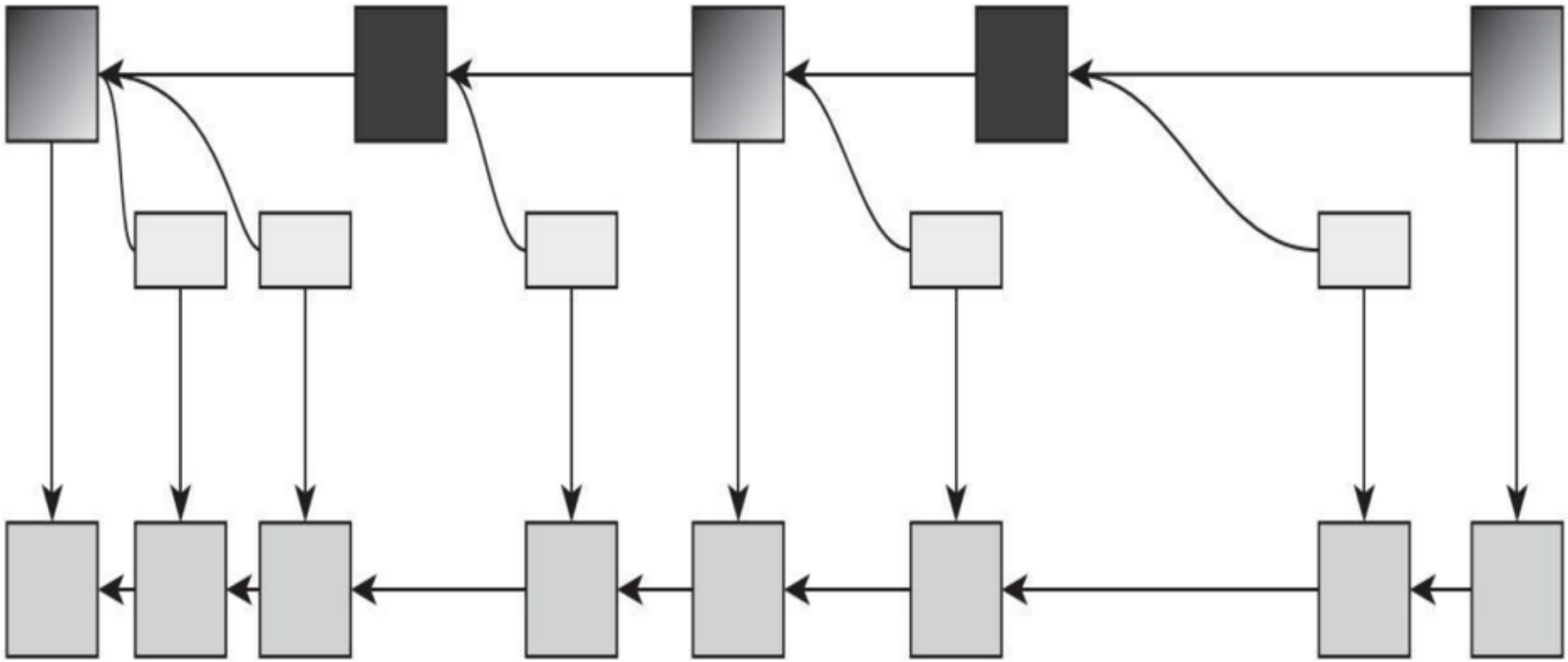
拉高出货

初始分配

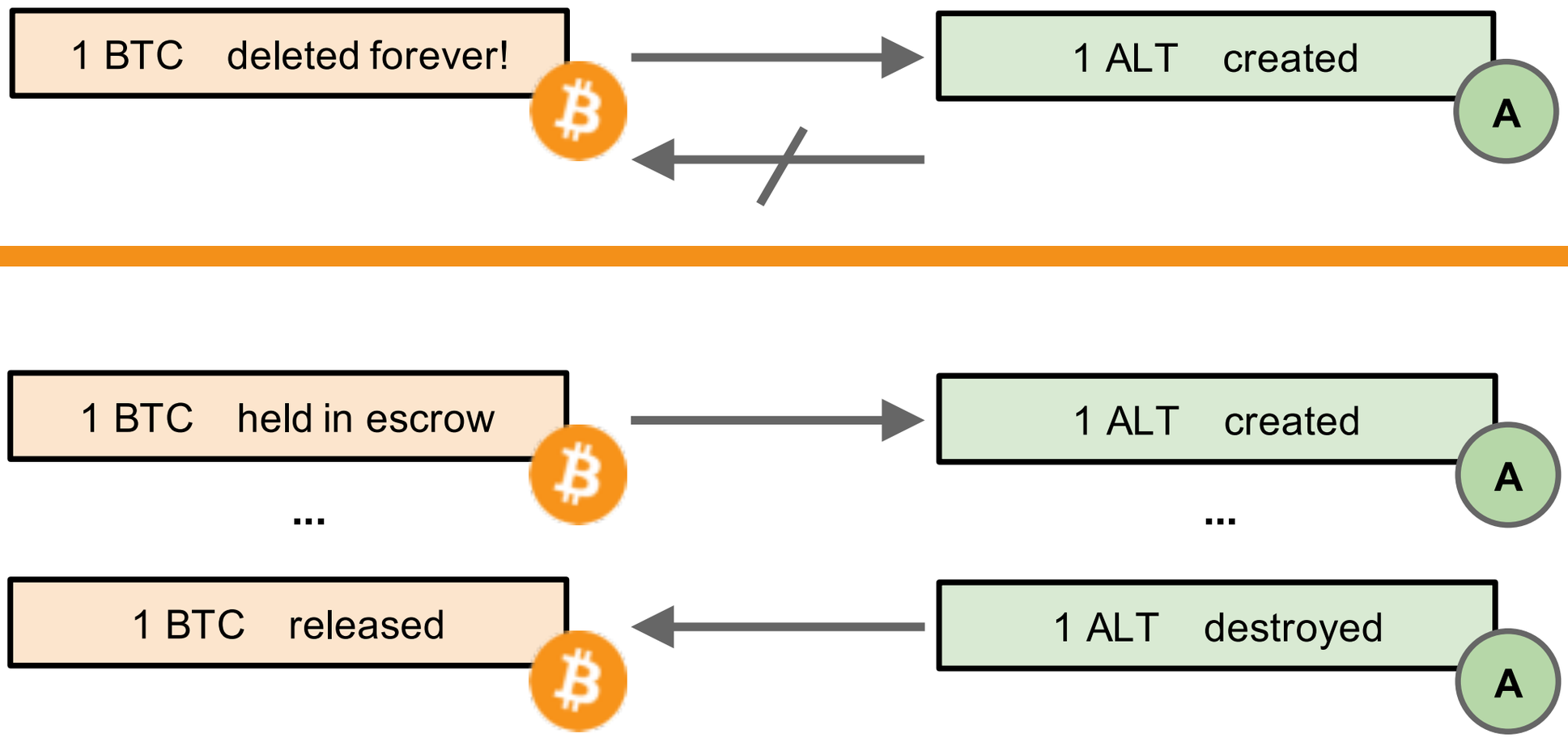
挖矿攻击

共同挖矿

共同挖矿



侧链


1 BTC deleted forever!
1 ALT created
A
1 BTC held in escrow
1 ALT created
A
...
...
1 BTC released
1 ALT destroyed
A

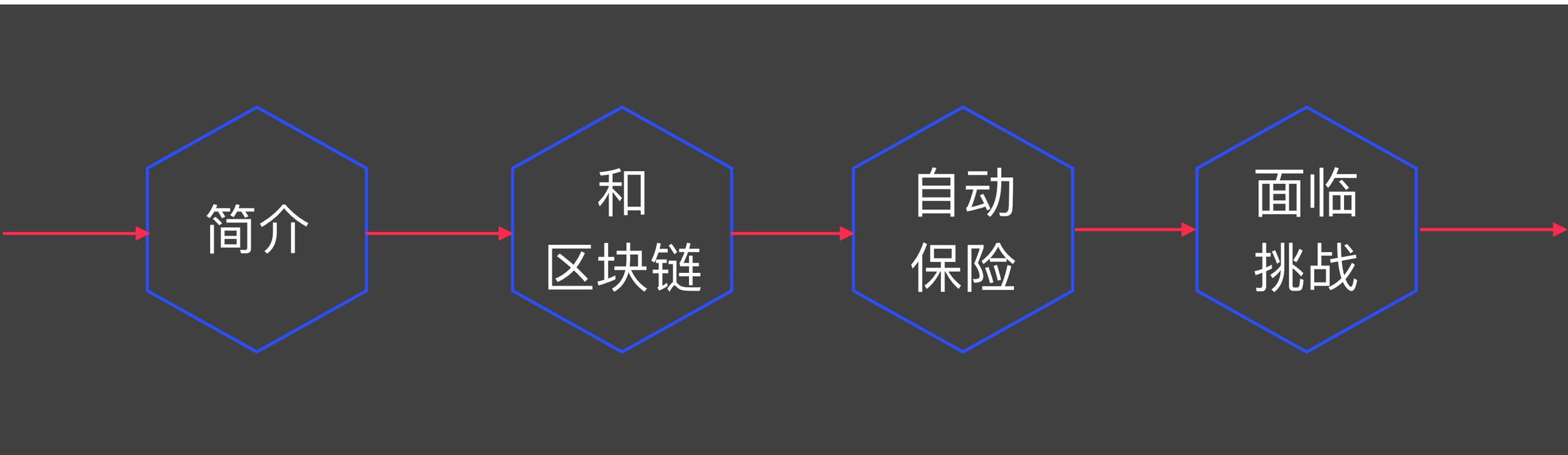

00001010
00000010
00001110
00000110

更多的链正在路上

ethereum

HYPERLEDGER

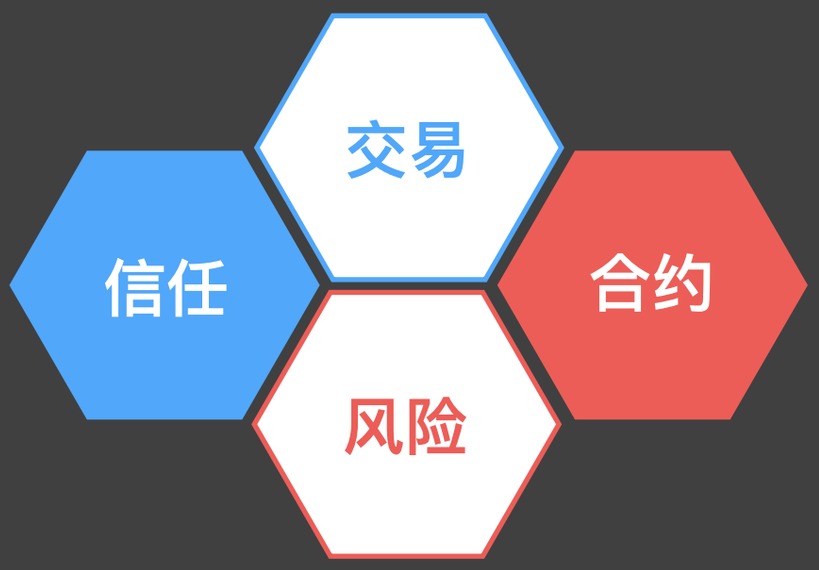
智能合约



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 Applications

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

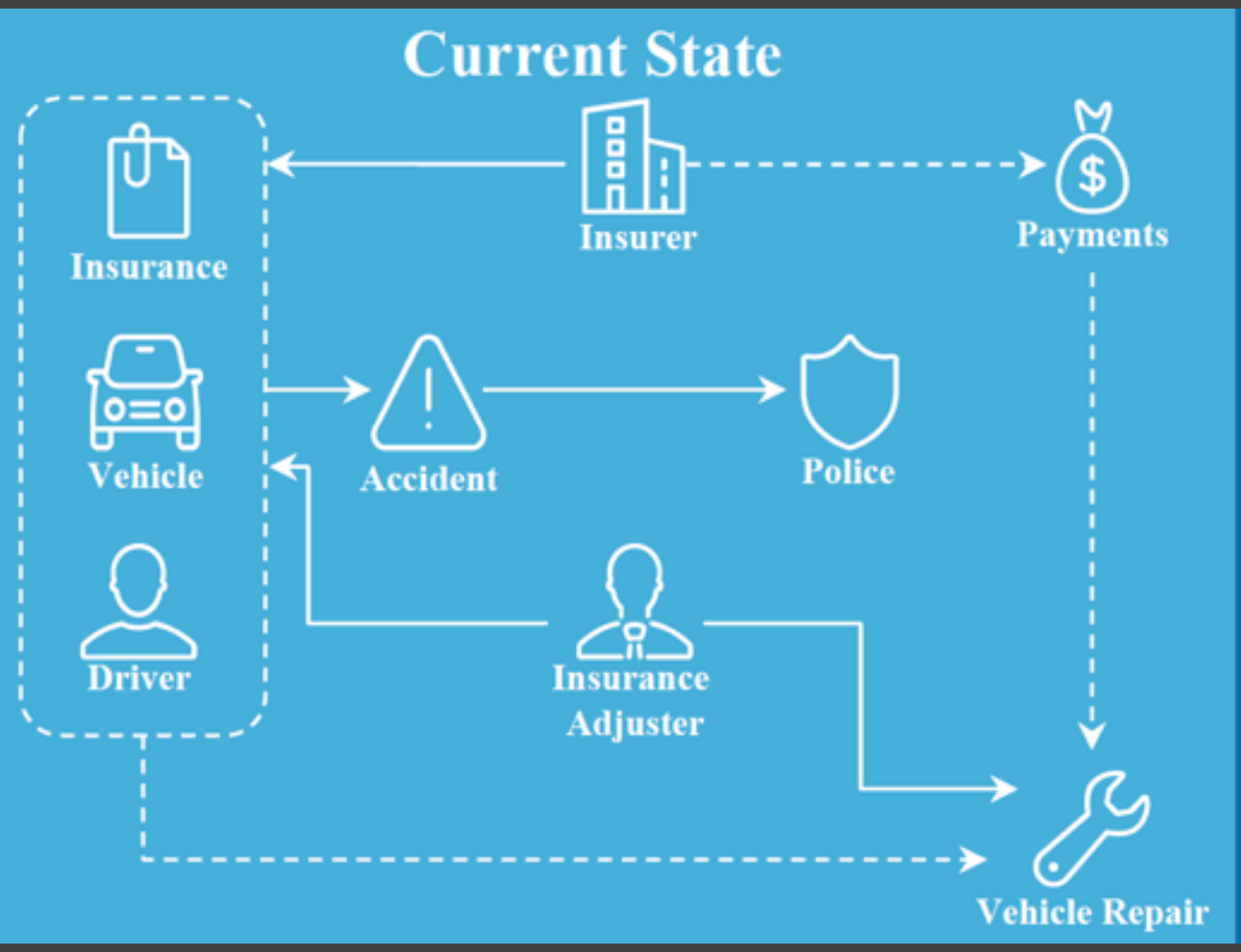
智能合约在区块链上存储并执行

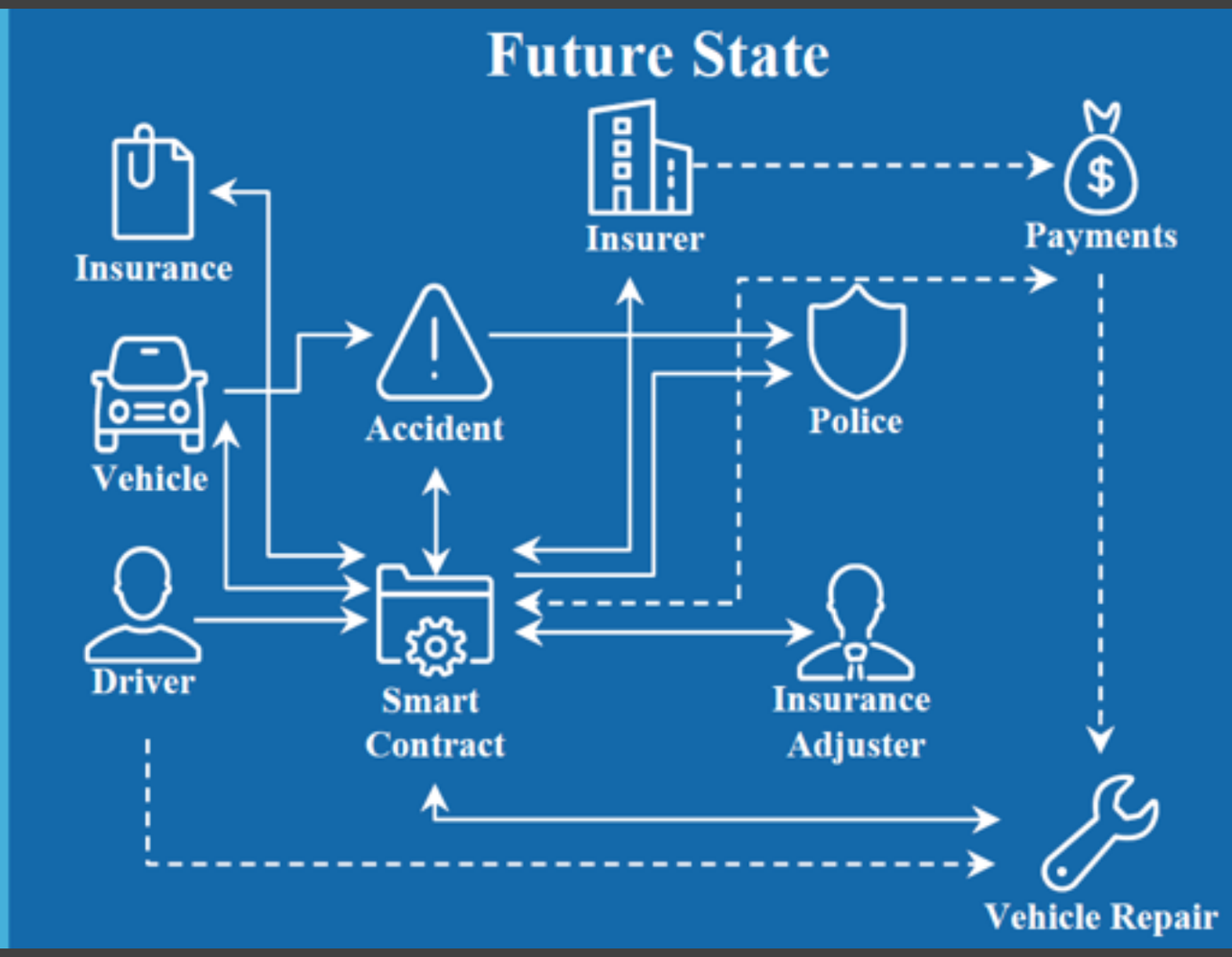
Block #FCAC
prev #618C
</> contract 2E12...
</> contract FECB...
</> contract 21E0...
...

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

Block #5
prev #5
</> con
</> con
</> con
...

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

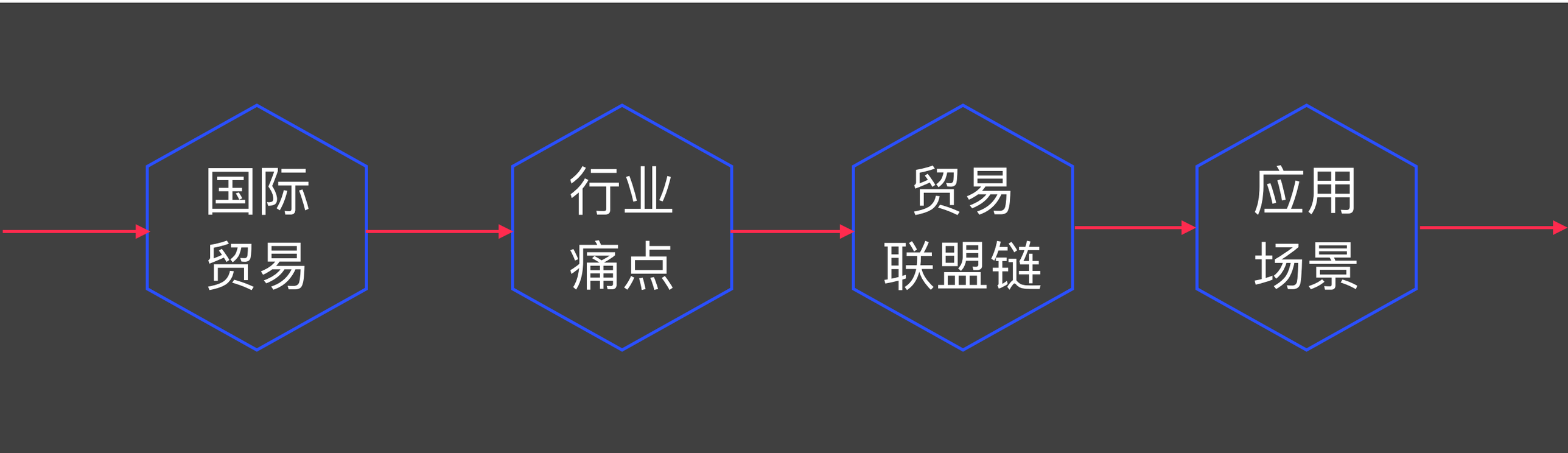
安全

- 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

国际贸易应用



Blockchain Applications

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
Applications

应用场景

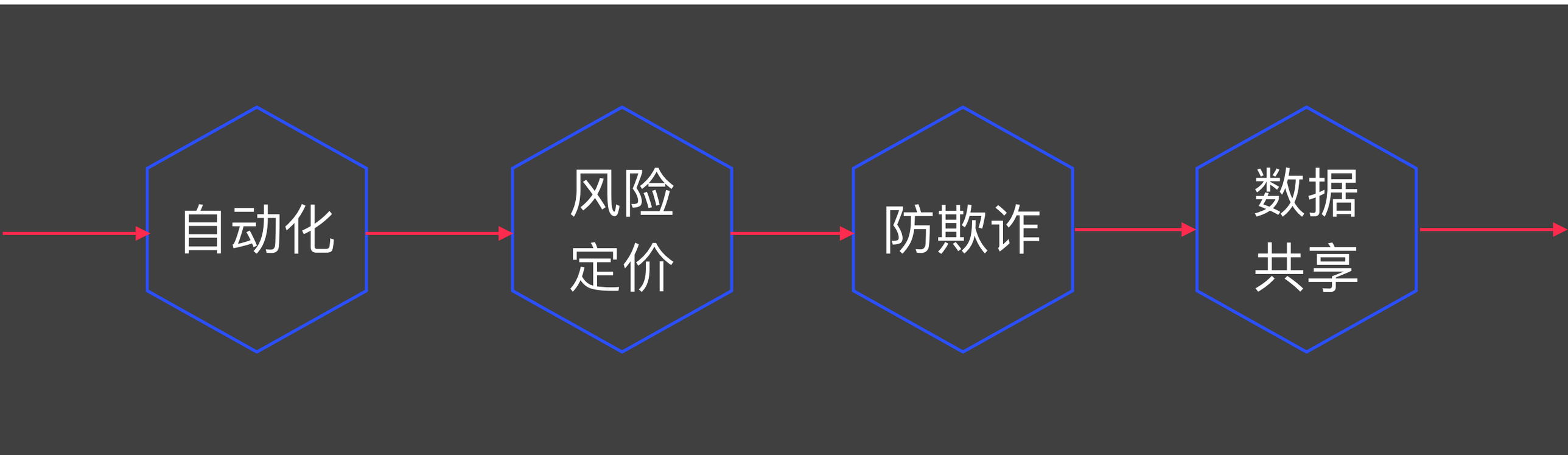
使用区块链来更新改造传统的外贸信用证、外贸保函、福费廷、保理和票据等业务。

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。

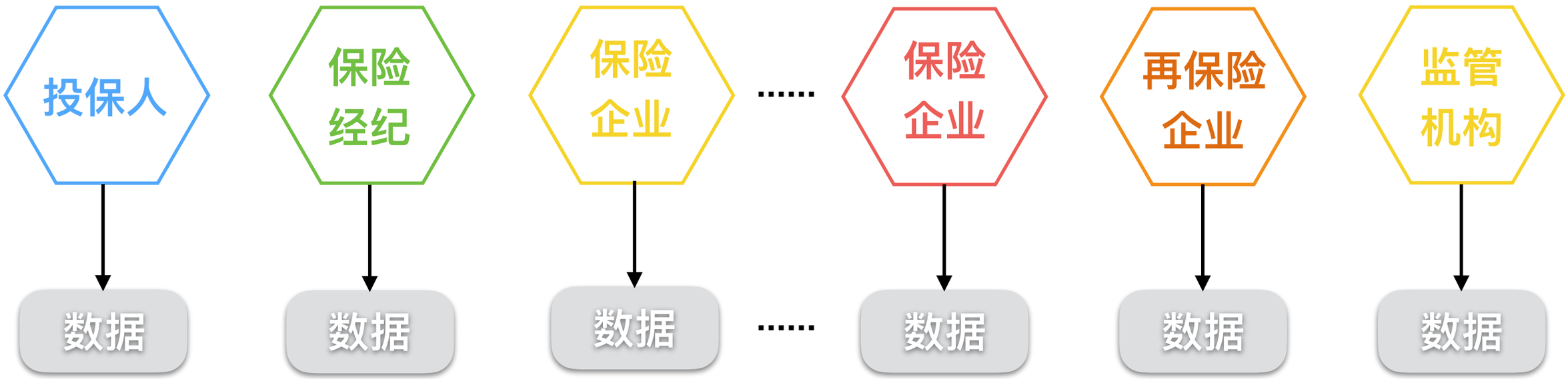
基于采集到的国际贸易供应链数据，使用专门为国际贸易定制的风控模型和算法，为企业画像，智能评估企业信用，减少欺诈行为，降低风险。

保险应用



Blockchain Applications

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

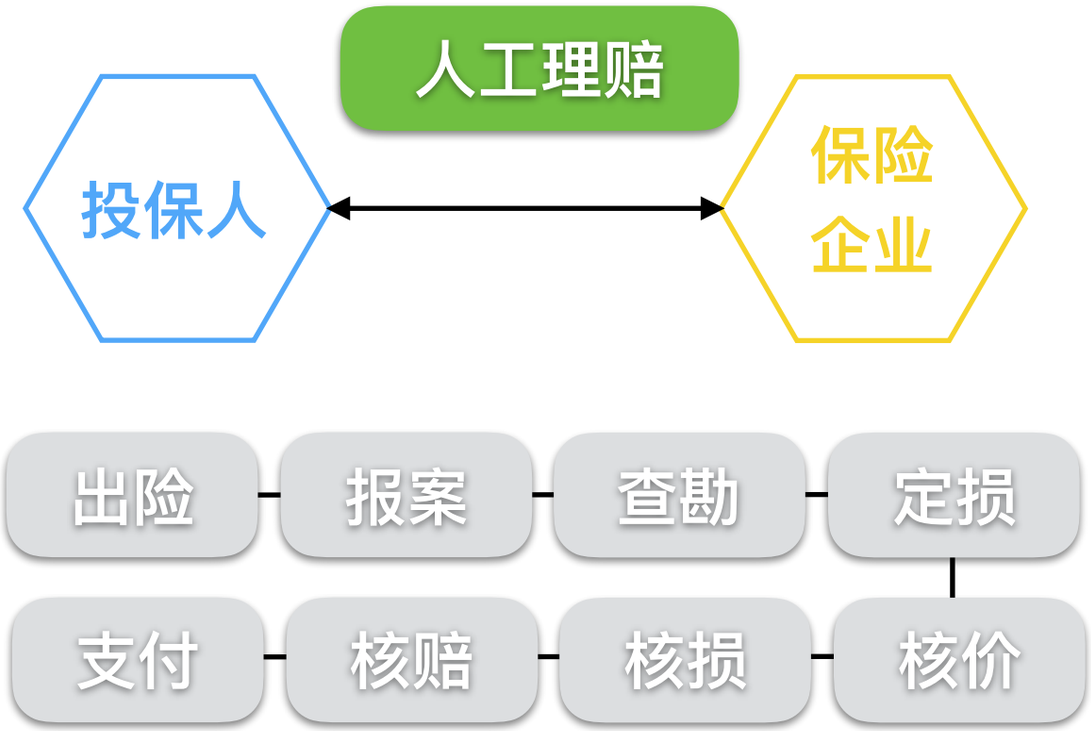
AI

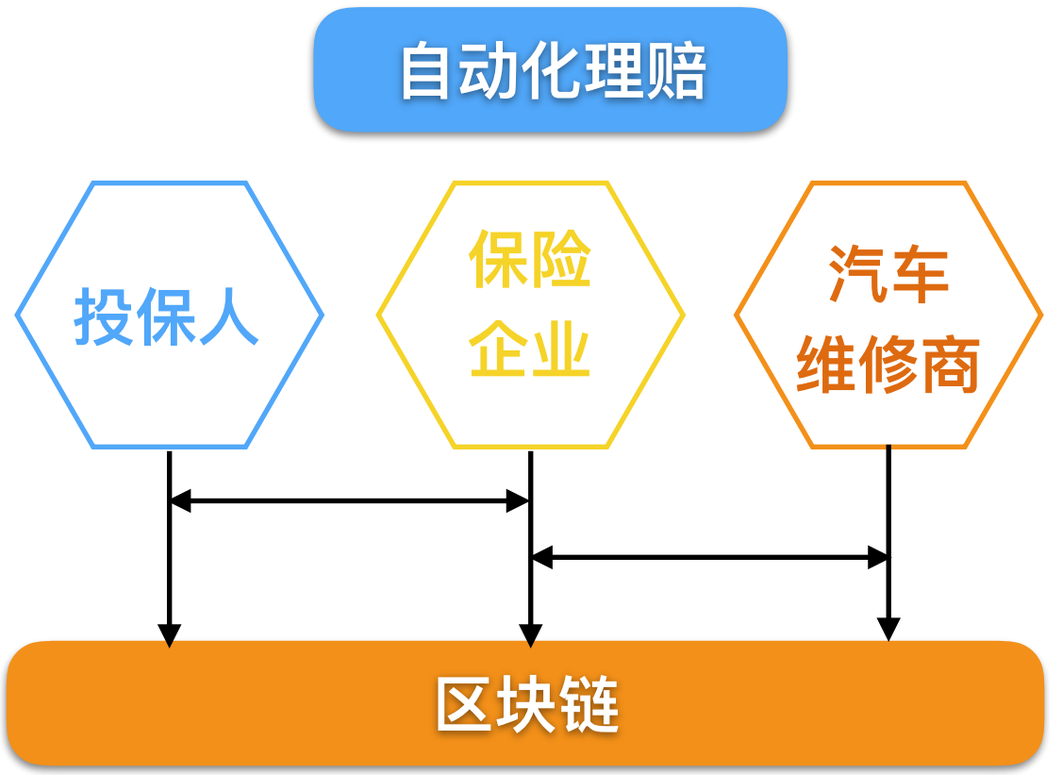
BigData

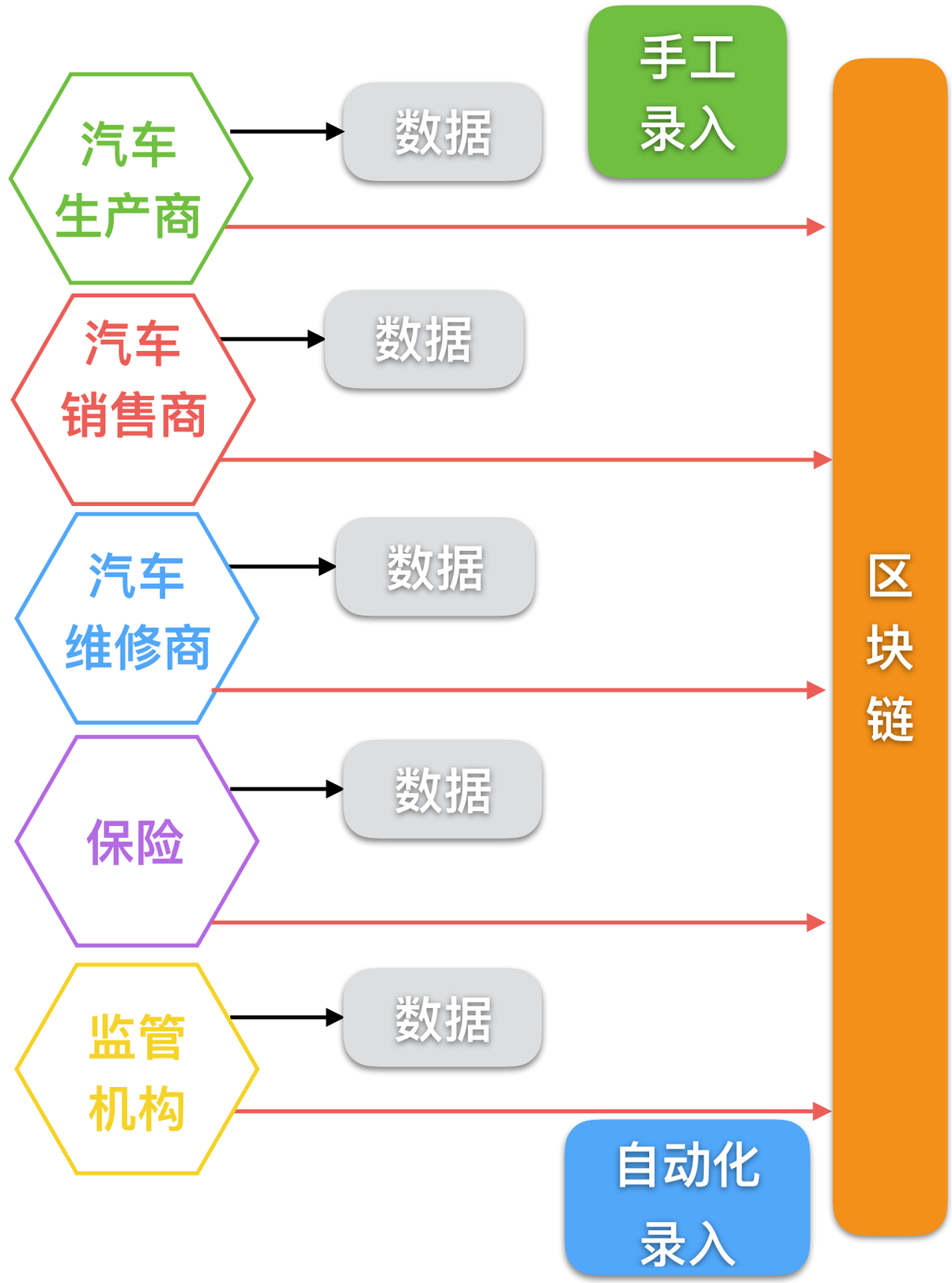
Cloud

Blockchain

自动化

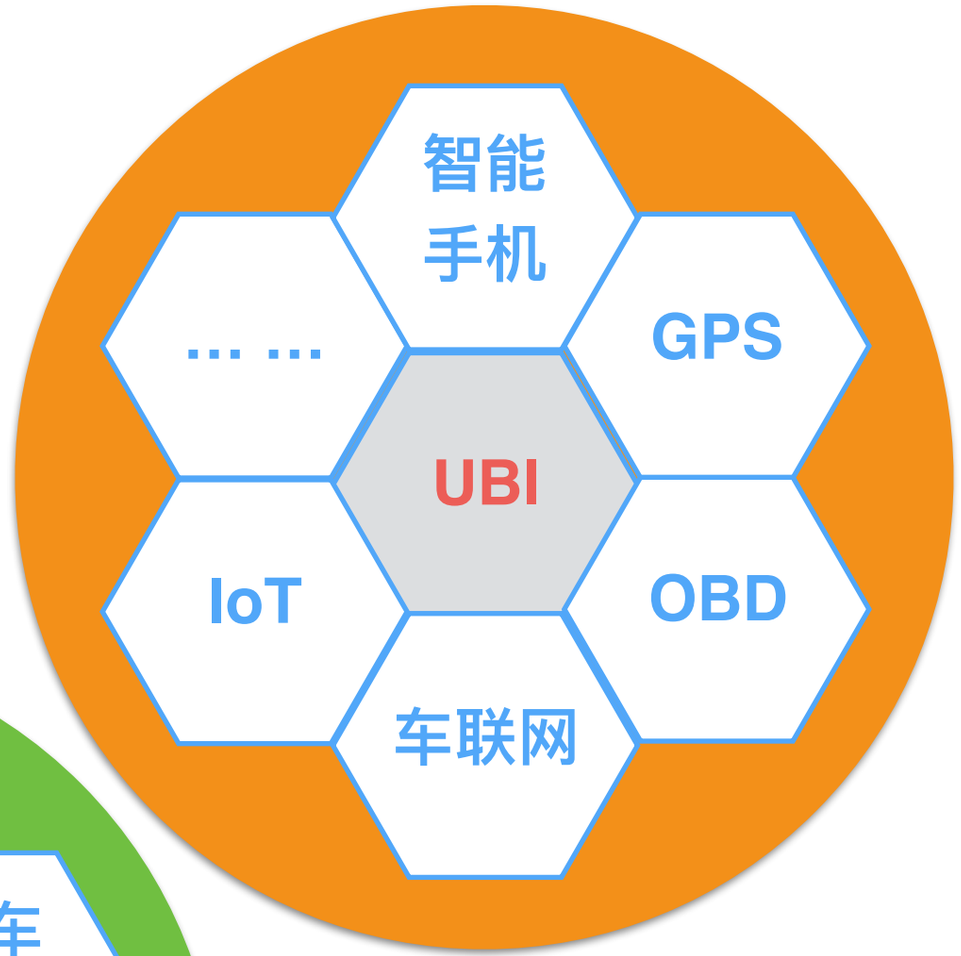

人工理赔
投保人
保险企业
出险
报案
查勘
定损
支付
核赔
核损
核价


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

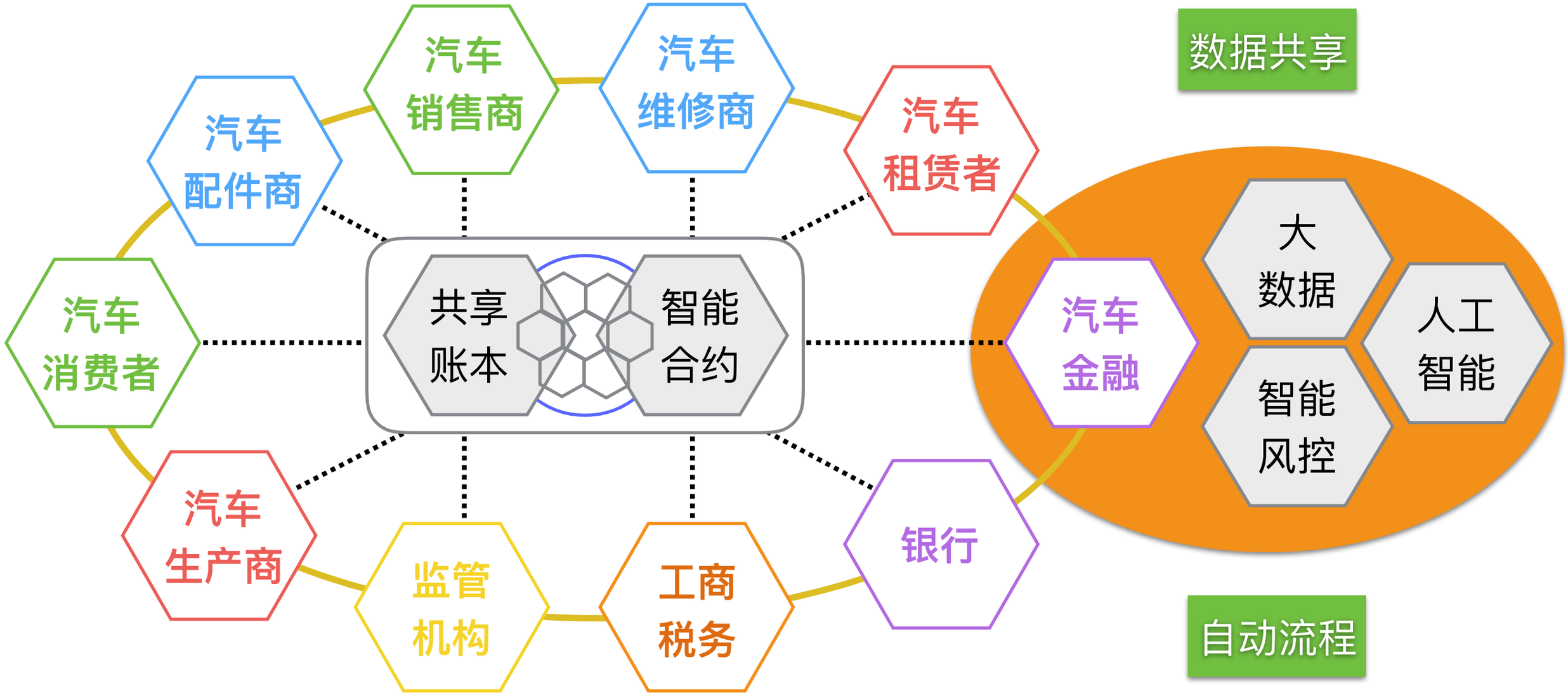
定价


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

防欺诈



基于多来源数据
比对防欺诈

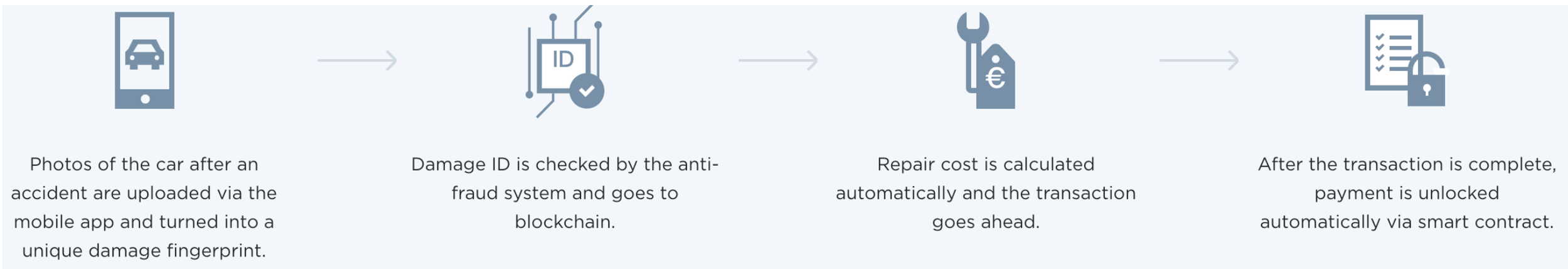
基于自动化和智能
合约防欺诈

Kasko2go

- 发生事故后向保险公司申请
- 保险公司进行伤害评估
- 司机等候保险公司分析
- 司机得到赔偿
- 通常需要很长时间

Kasko2go

- 事故发生后汽车的照片通过移动应用程序上传，并变成一个独特的损坏指纹；
- 损害ID由反欺诈系统检查并发送到我们的系统；
- 维修成本自动计算，交易继续进行；
- 交易完成后，通过智能合约自动解锁付款；
- 30分钟就能理赔成功。



Kasko2go

- 动态评估驾驶条件和事故风险：通过分析驾驶员的行为，选定的路线，事故率，天气条件和其他特征，为每个客户提供个性化的方法。不使用汽车时没有付款。保险范围是每分钟，每公里或每天。订阅方便，使用方便。移动应用程序是免费的，不需要额外的设备。
- 反欺诈系统：通过使用来自任何数码相机的单张照片，公司会标记有损坏的汽车的每一部分并将其转换为独特的数字签名。然后，它会将唯一的签名与损害赔偿库交叉核对，澄清损害是否已被声明或是否故意增加了损害。这允许检测受损部件的多次使用和夸大的声明，并对欺诈行为发出警报。

Kasko2go

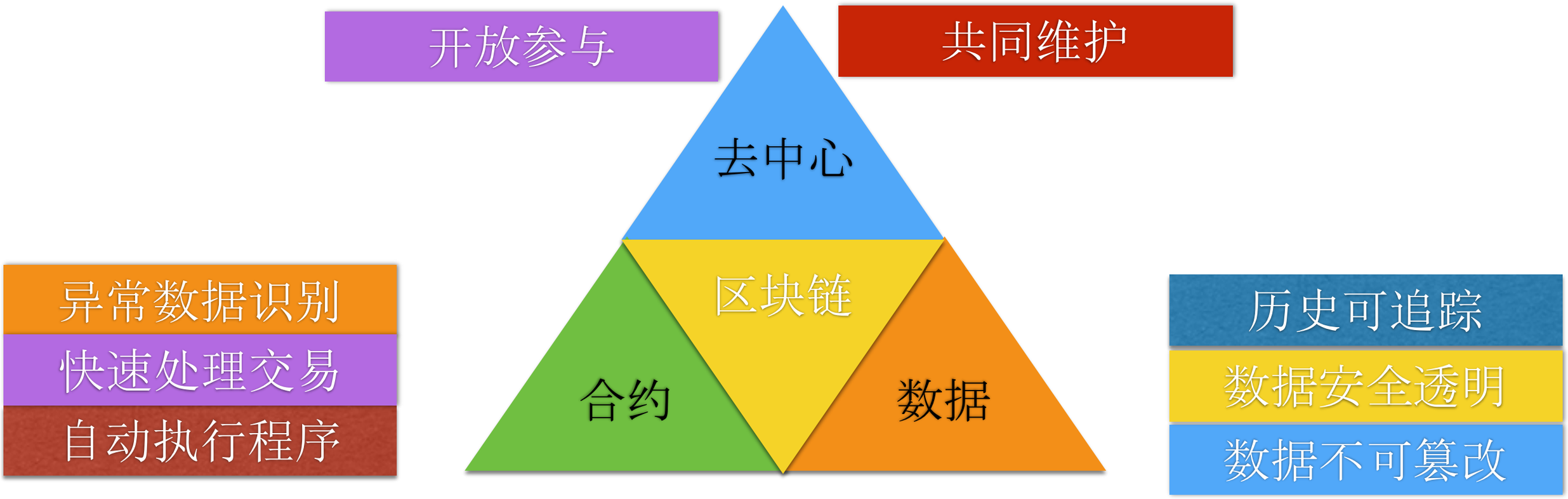
- 价格透明度,
- 个人对保险费率的控制,
- 较低的费率（与传统解决方案相比高达50％）， 特别是对于年轻车手和低里程驾驶员,
- 与家人，朋友等共享汽车的驾驶员的灵活性,
- 青少年父母和老人子女的“安心”,
- 更高的整体安全性：改善驾驶，减少事故频率和严重程度,
- 更快的事故协助和支持
- 忠诚度奖励。

Kasko2go

- 更好的风险管理和控制，
- 通过个性化的即用即付优惠吸引新的低风险客户，增加客户群，
- 降低索赔损失 - 与提供传统解决方案的保险公司相比，减少高达30％，
- 欺诈检测和欺诈成本（减少索赔处理成本 - 减少高达55％），
- 更好的交互性和与客户的沟通，从而提高客户满意度，保留率和忠诚度。

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

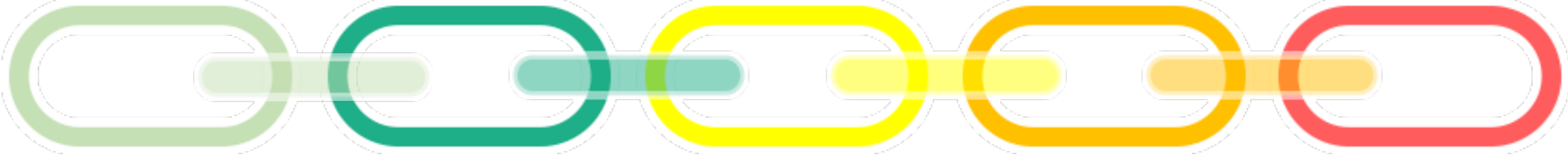

开放参与
共同维护
去中心
区块链
合约
数据
异常数据识别
快速处理交易
自动执行程序
历史可追踪
数据安全透明
数据不可篡改

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。

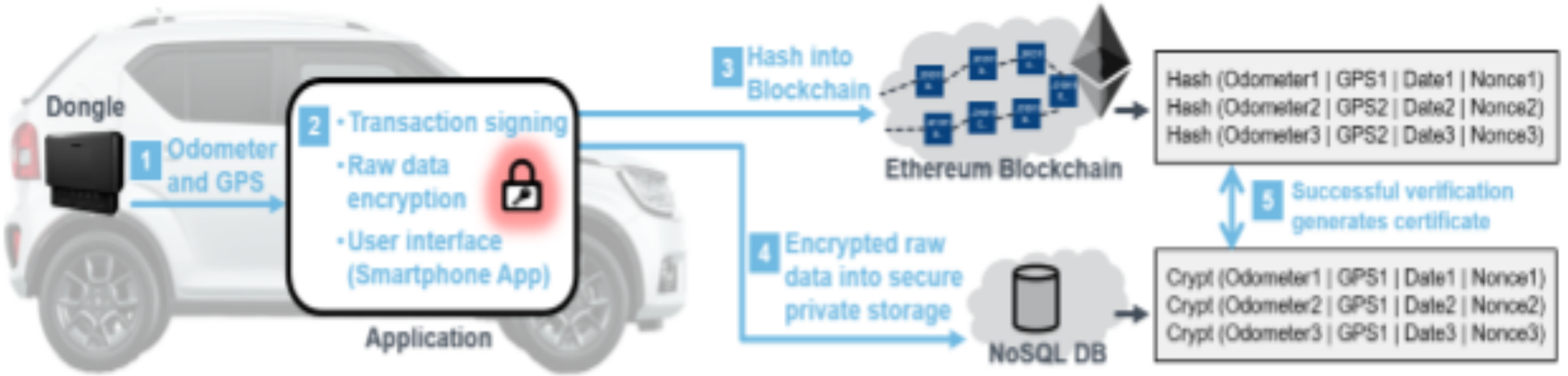
保险公司：保险公司拥有汽车保险信息，以及通过保险理赔的事故信息和维修记录。

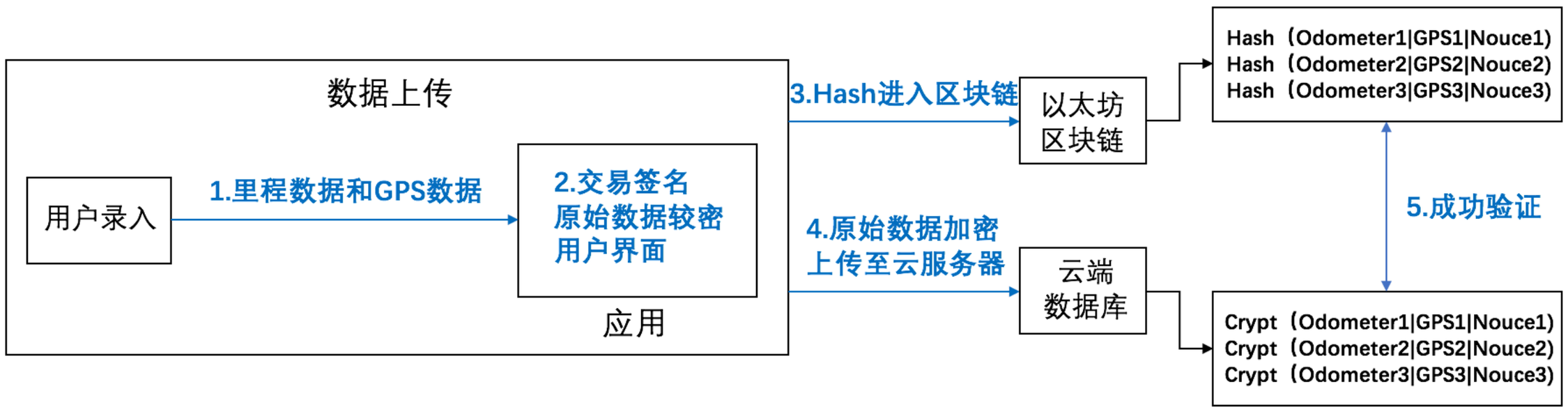


汽车使用者：通过车载远程设备是记录汽车数据，主动规律得上传汽车的使用情况，比如里程、gps、油耗、车速等。或允许用户手动录入。

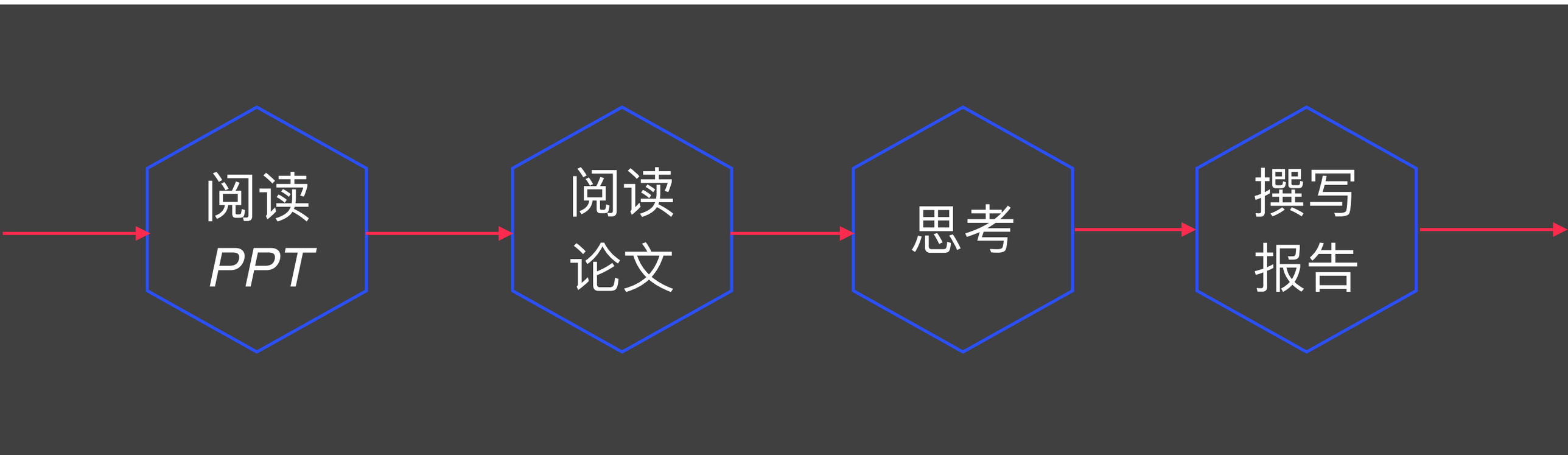
汽车服务商和服务站：汽车在进行维修时，维修站向相关部门提交汽车的数据，汽车服务商收集的数据，可以与其它渠道的数据相互印证。

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)
5 Successful verification generates certificate
4 Encrypted raw data into secure private storage
NoSQL DB
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)

课后作业



Homework

课后作业

基于Bitcoin开发一个应用

1、基于Bitcoin开源库

2、实现一个常见的应用

3、可以运行，可以演示

4、可以改造Bitcoin

12月2日晚上12点前提交给助教

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io