区块链应用等

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

Course Overview

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

Course Overview

本次课程内容

1 应用

- 智能合约
- 面临挑战
- 国际贸易
- 保险

2 监管

- 共识
- 社区
- 分叉
- 政府

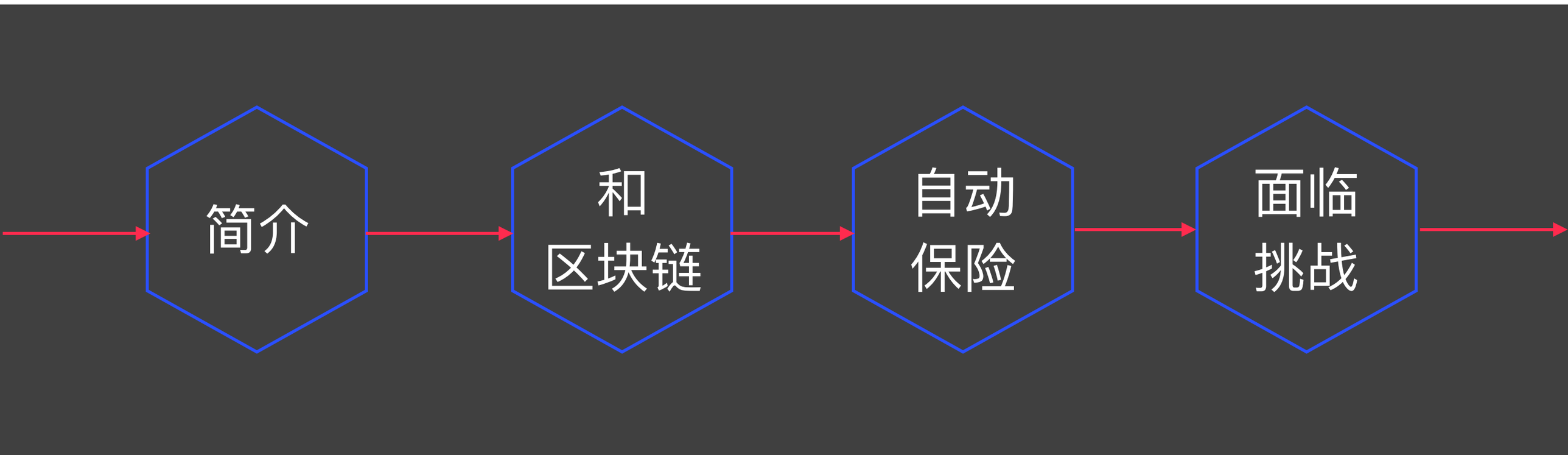
3 平台

- 平台
- 博彩
- 随机源
- 预测市场

4 代币

- 产生
- 例子
- 共同挖矿
- 侧链

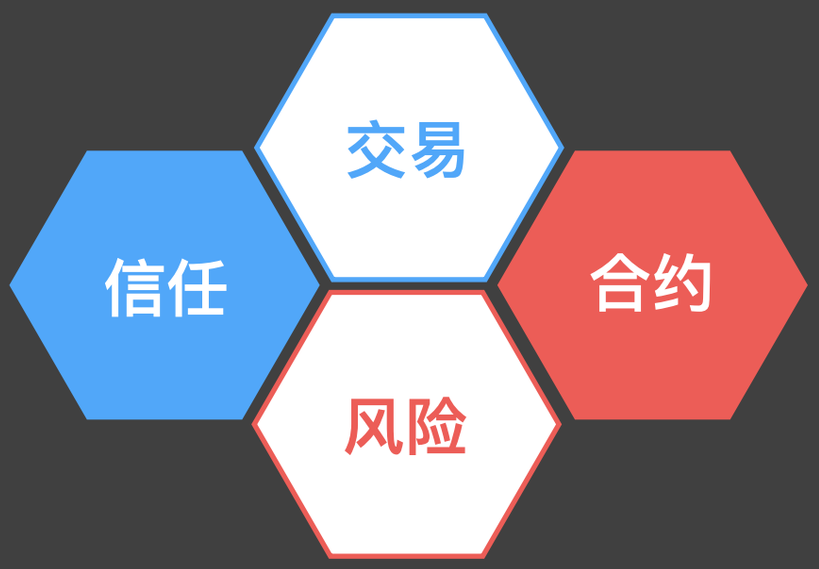
智能合约



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

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

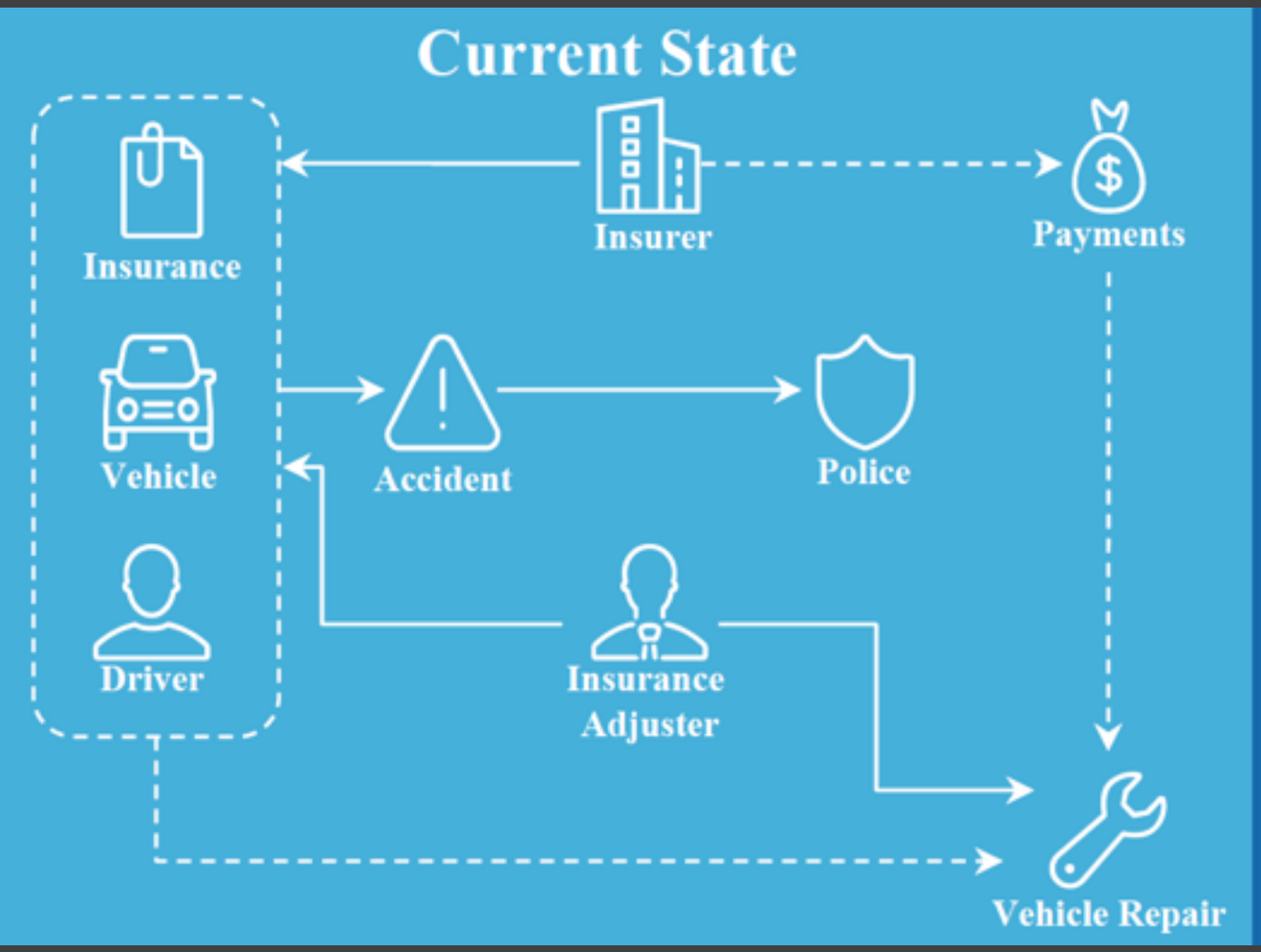
智能合约在区块链上存储并执行

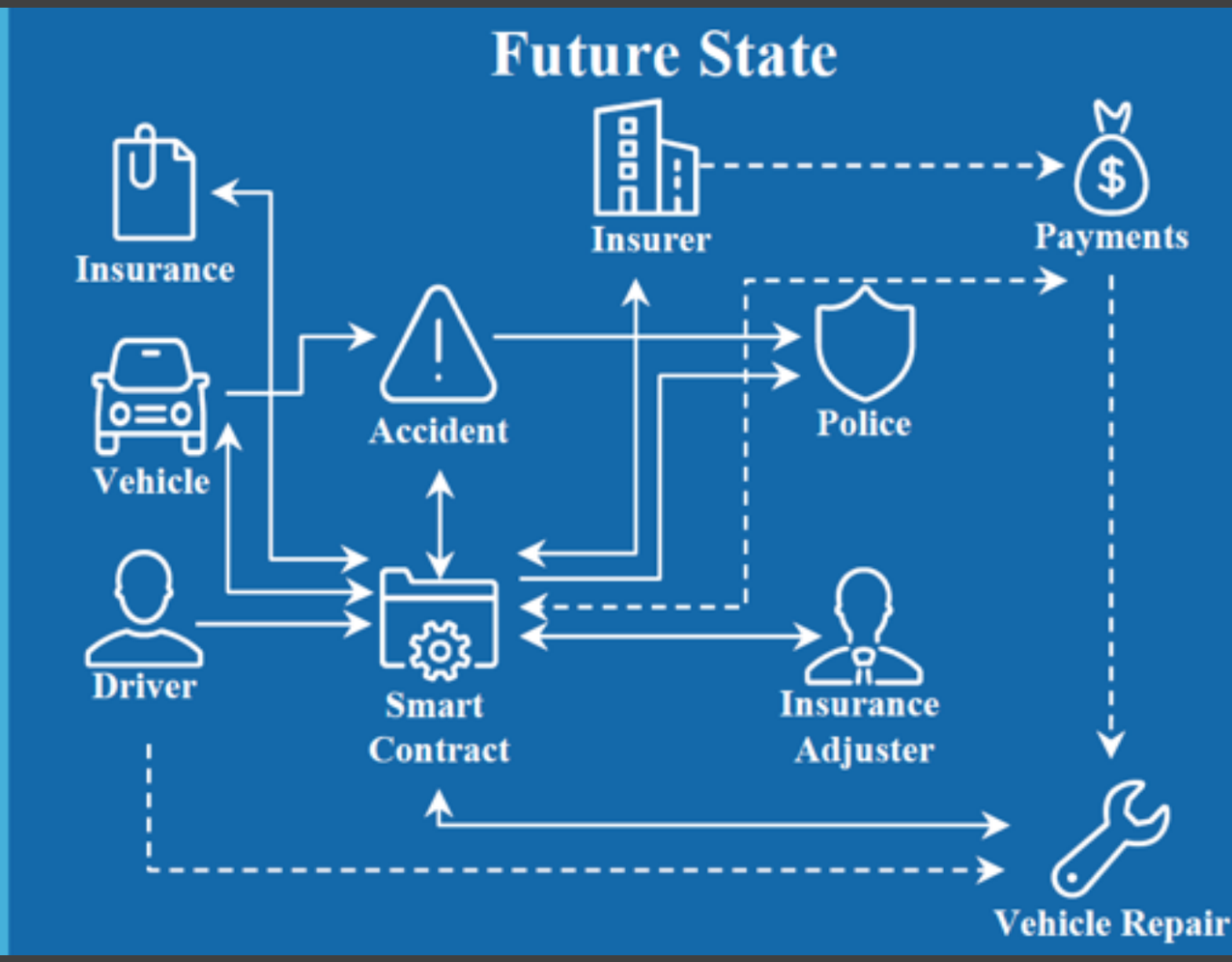
Block #FCAC
prev #618C
</> contract 2E12...
</> contract FECB...
</> contract 21E0...
...

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

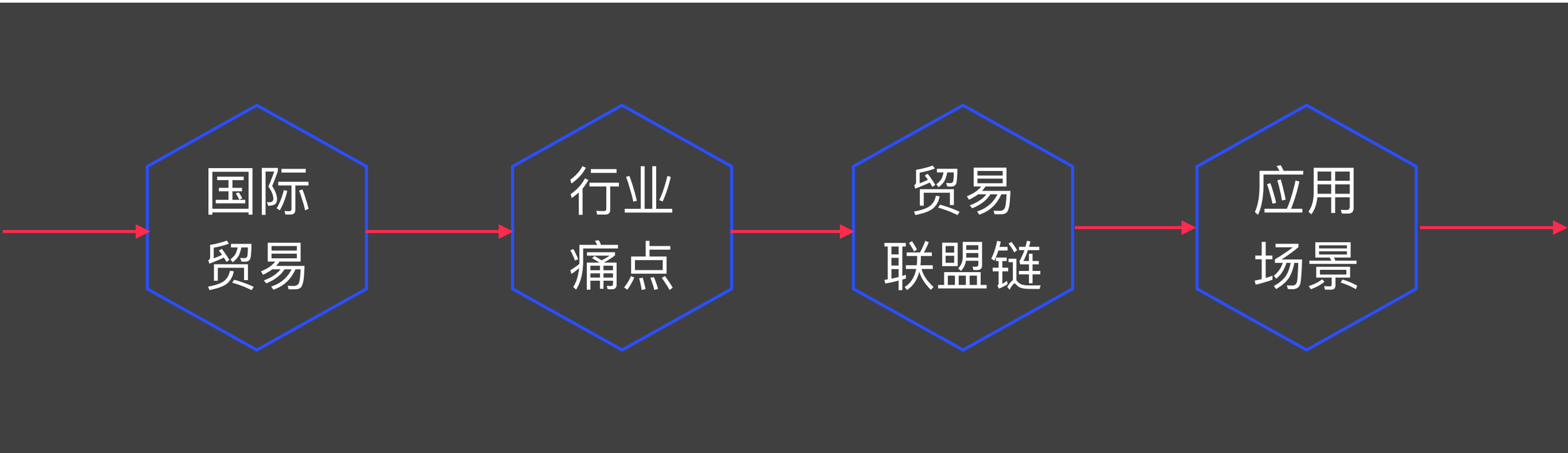
安全

- 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

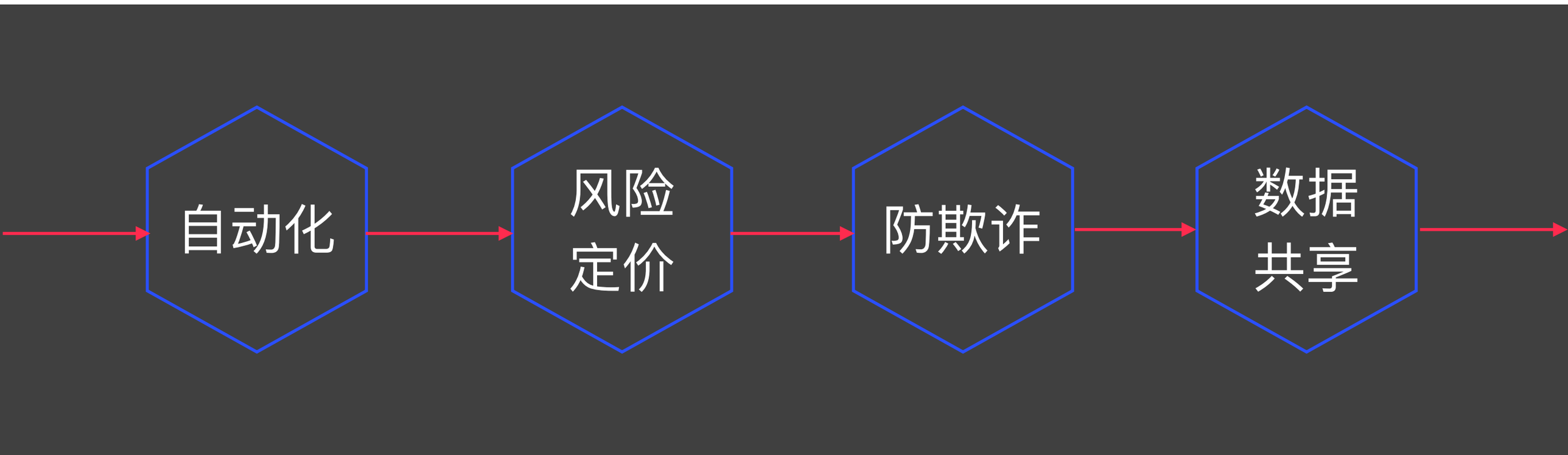
监管

- 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

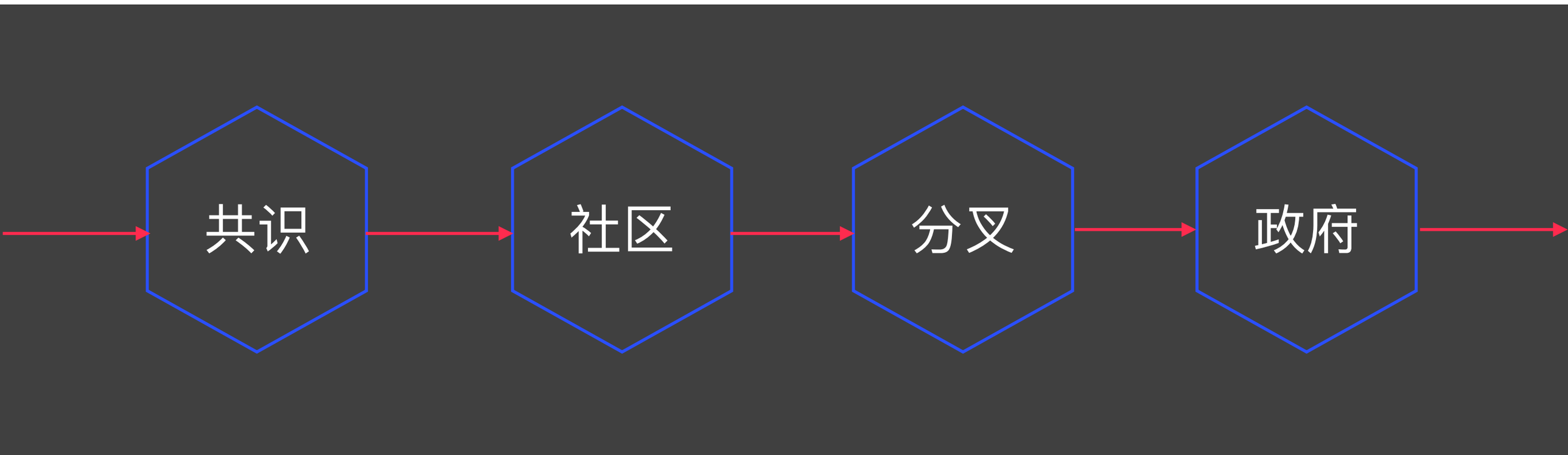
国际贸易应用



保险应用



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

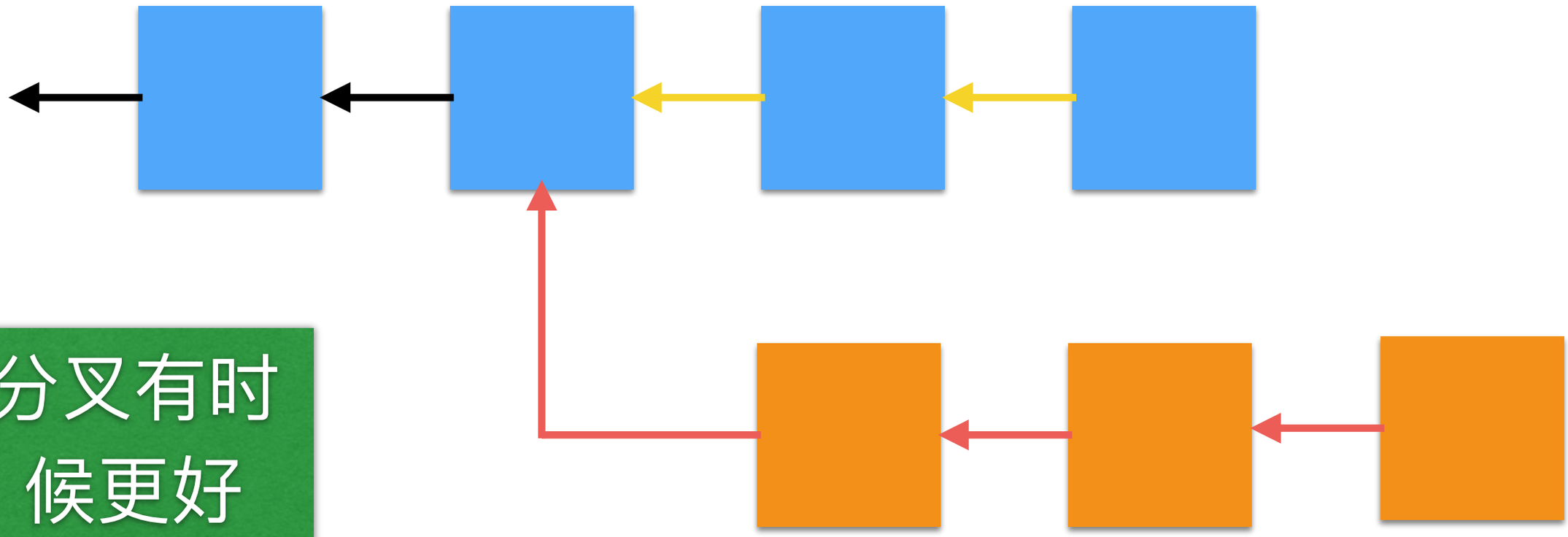
投资人：购买

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

纽约共识

SegWit

SegWit2x

BP141

BP91

BP148

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

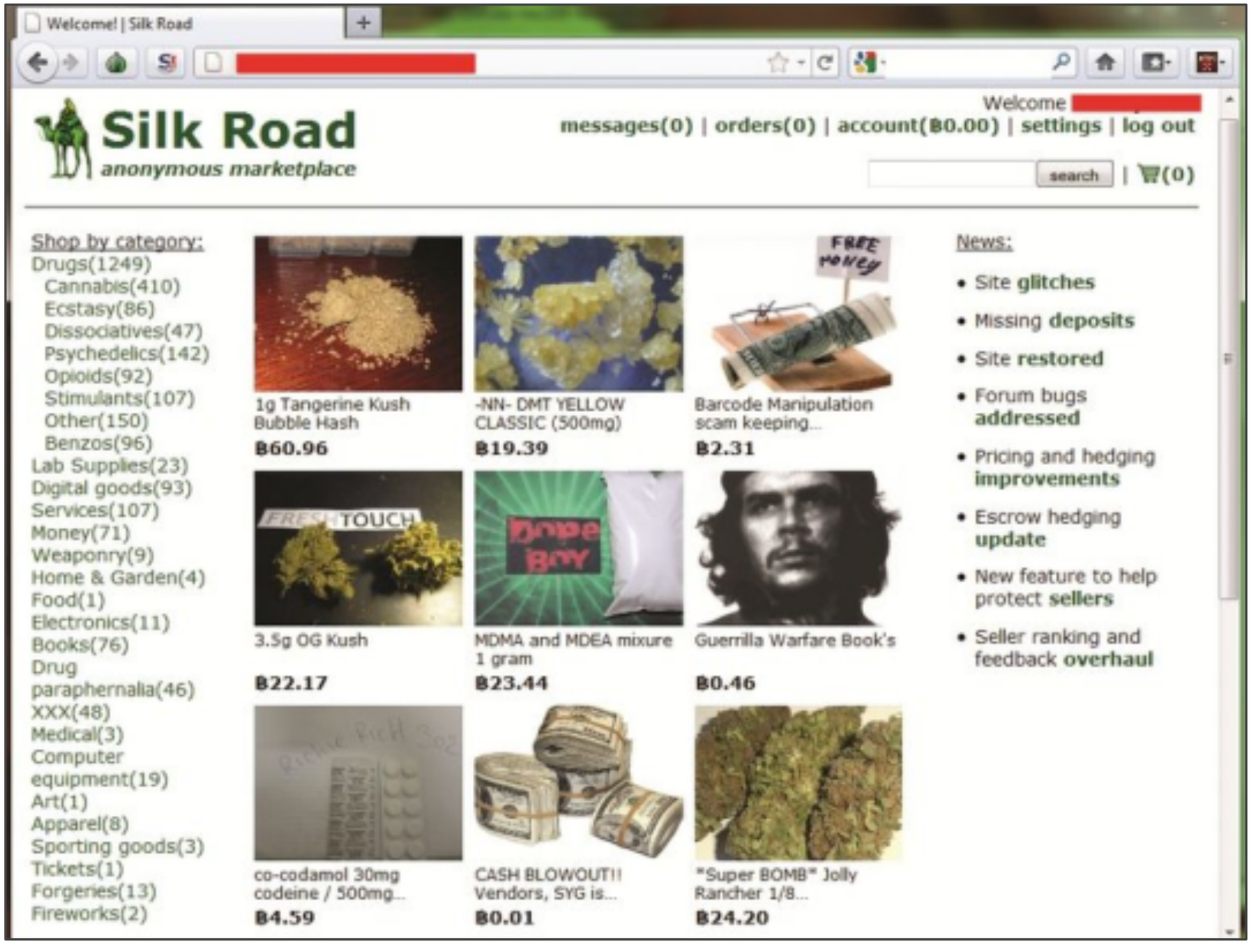
纽约州比特币牌照

美国加密货币管理政策

中国政府2017年系列政策

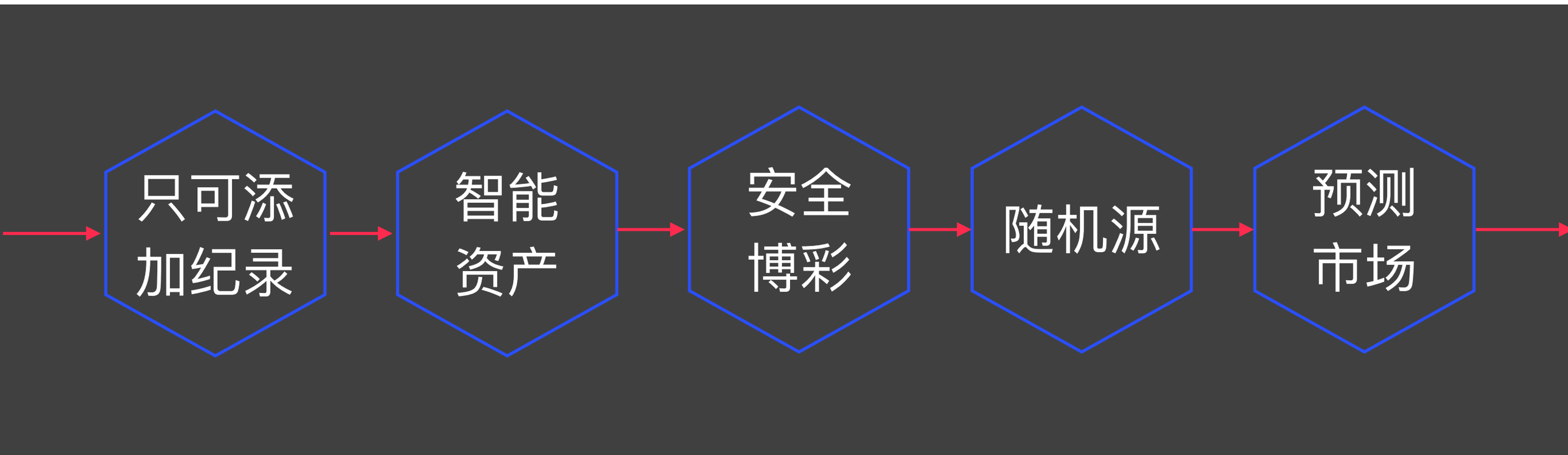
日韩
新加坡

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

Blockchain
Others

预测未来

FIFA2014

腐败指责

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

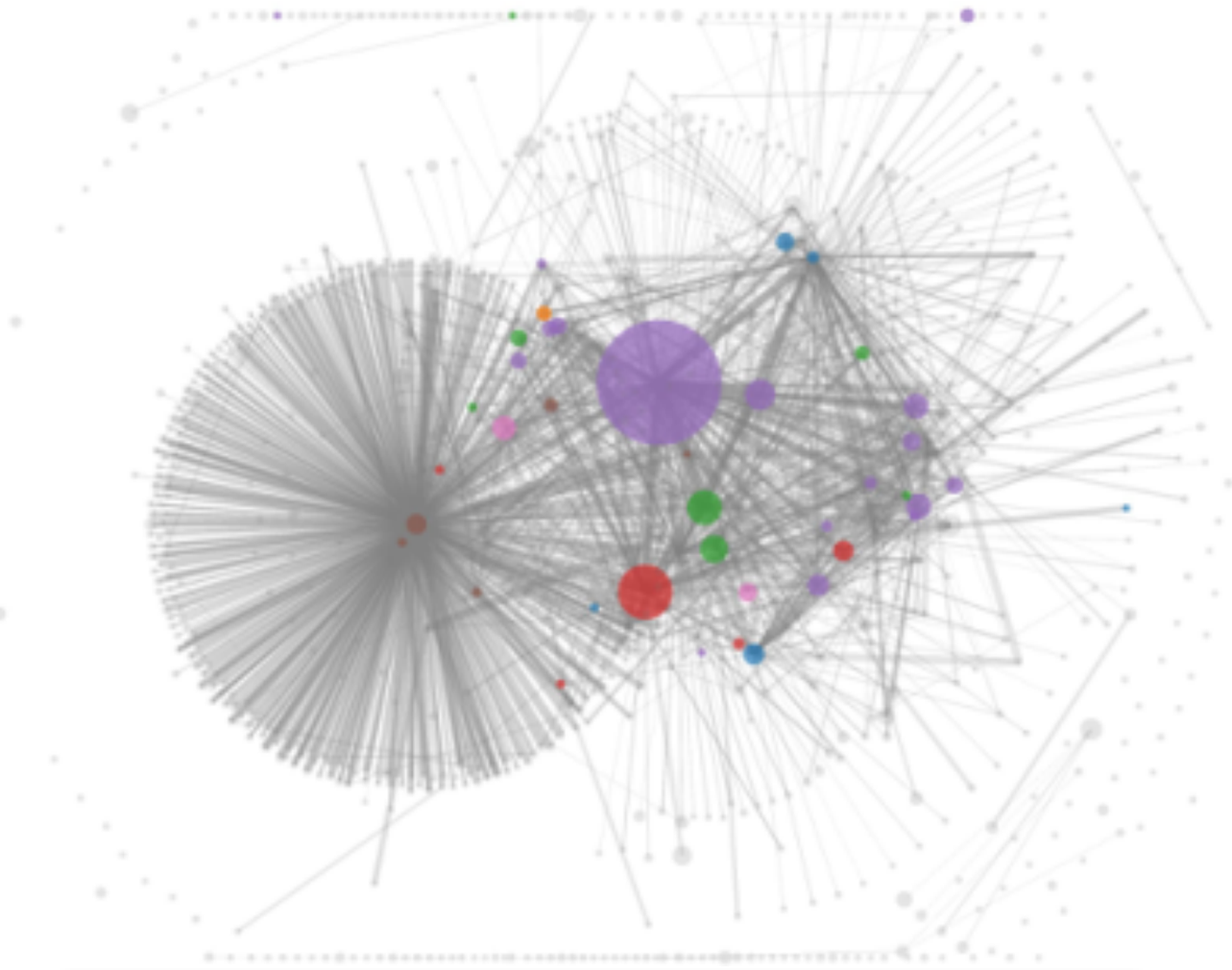
技术归技术

管理归管理

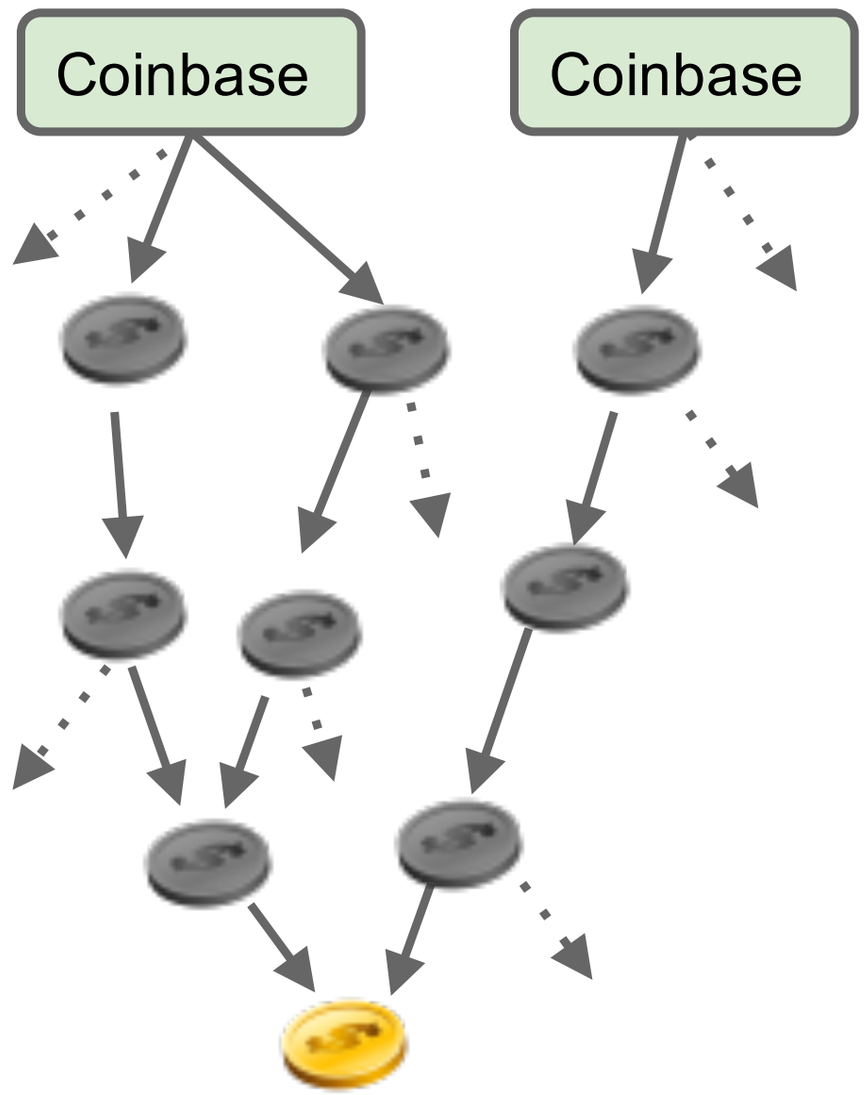
法律归法律

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

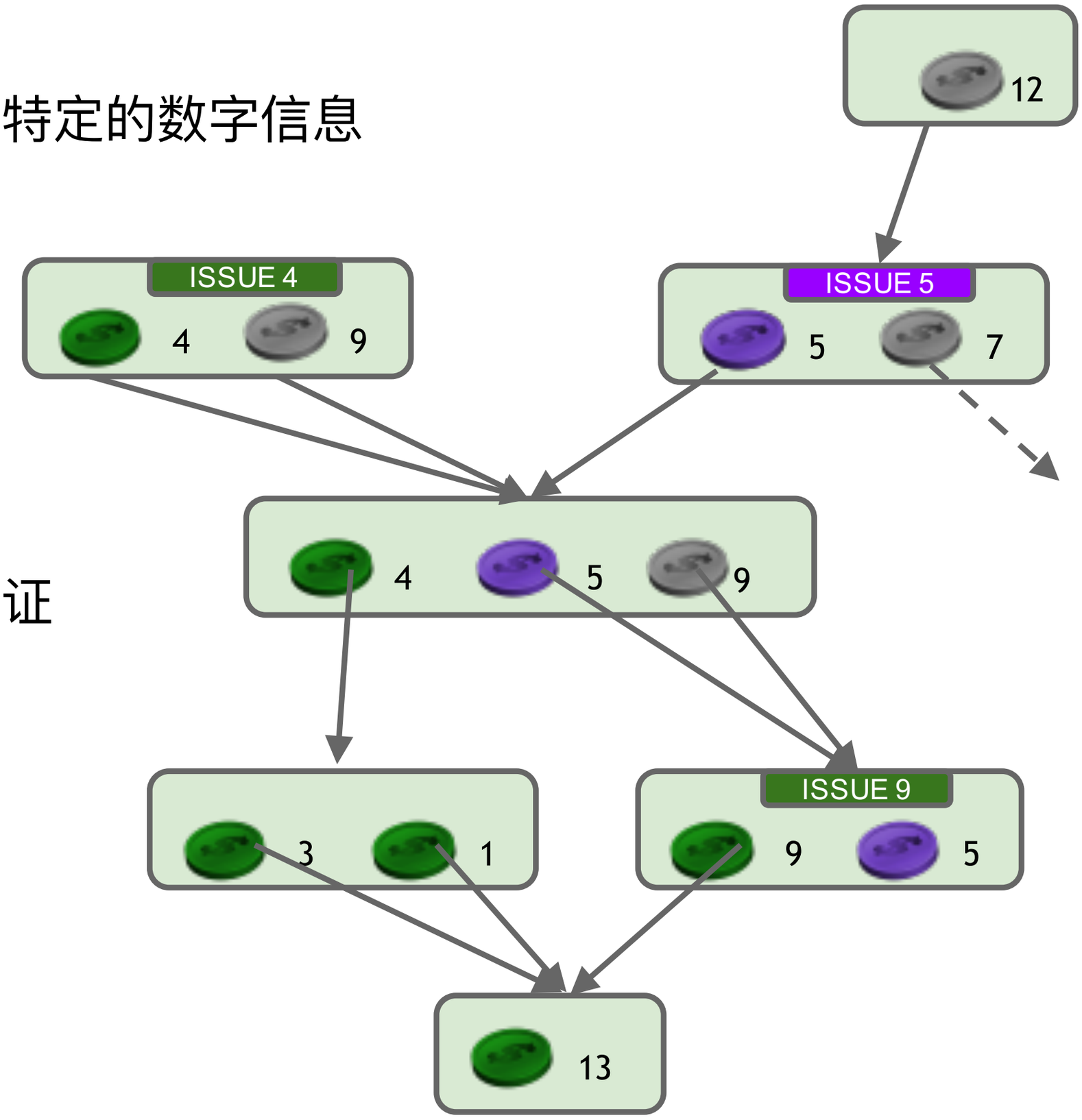
认证应用

"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

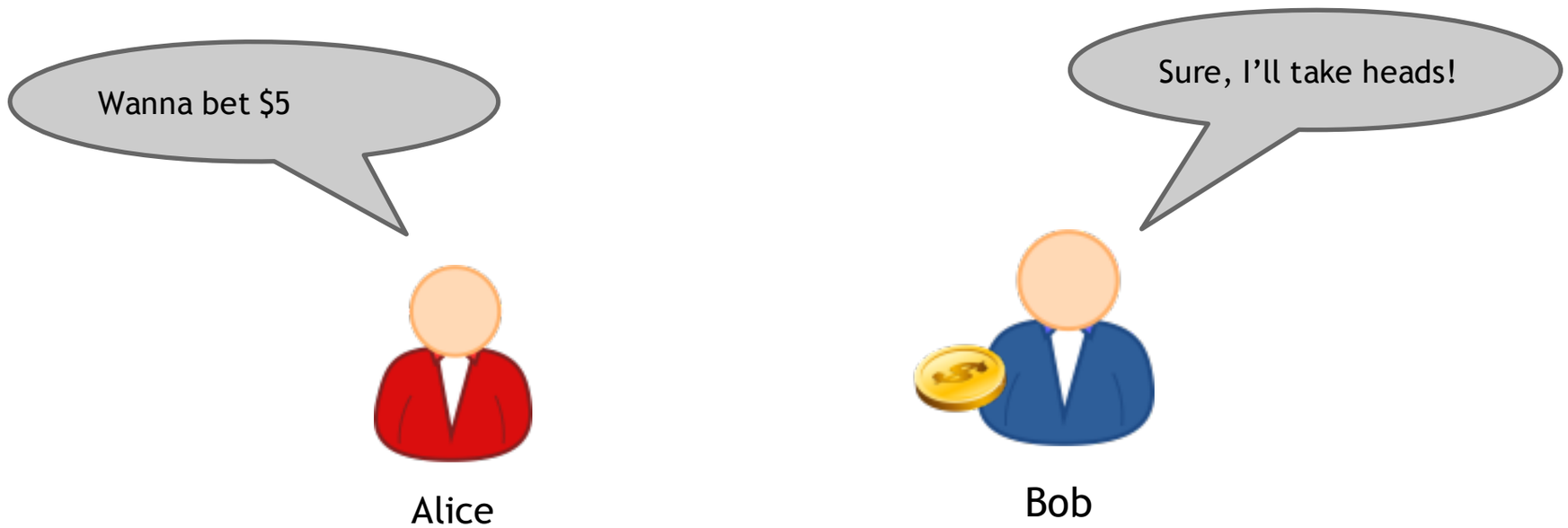
数字资产

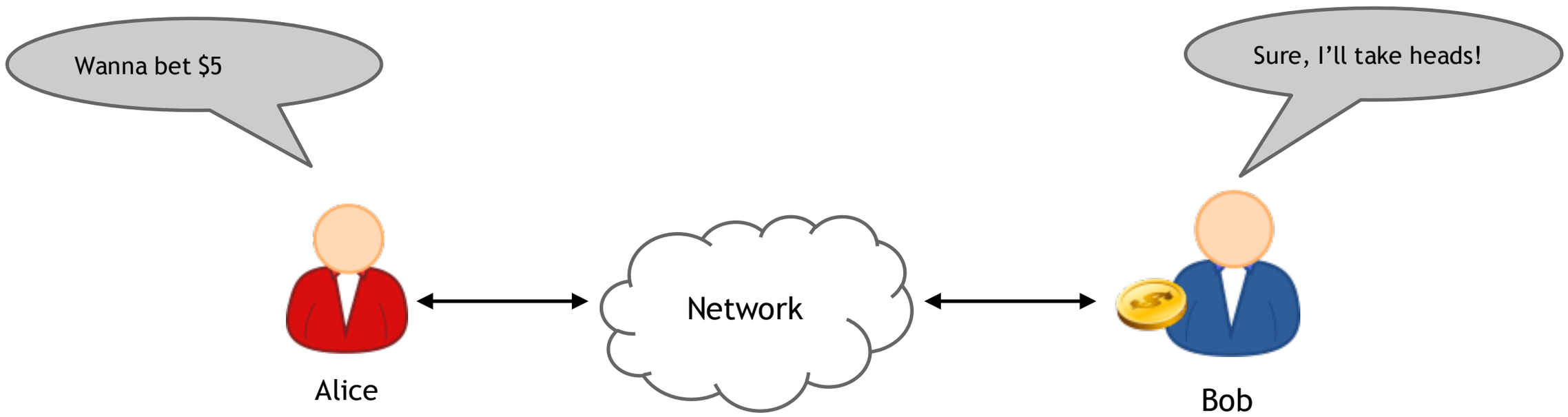
物理资产

股票

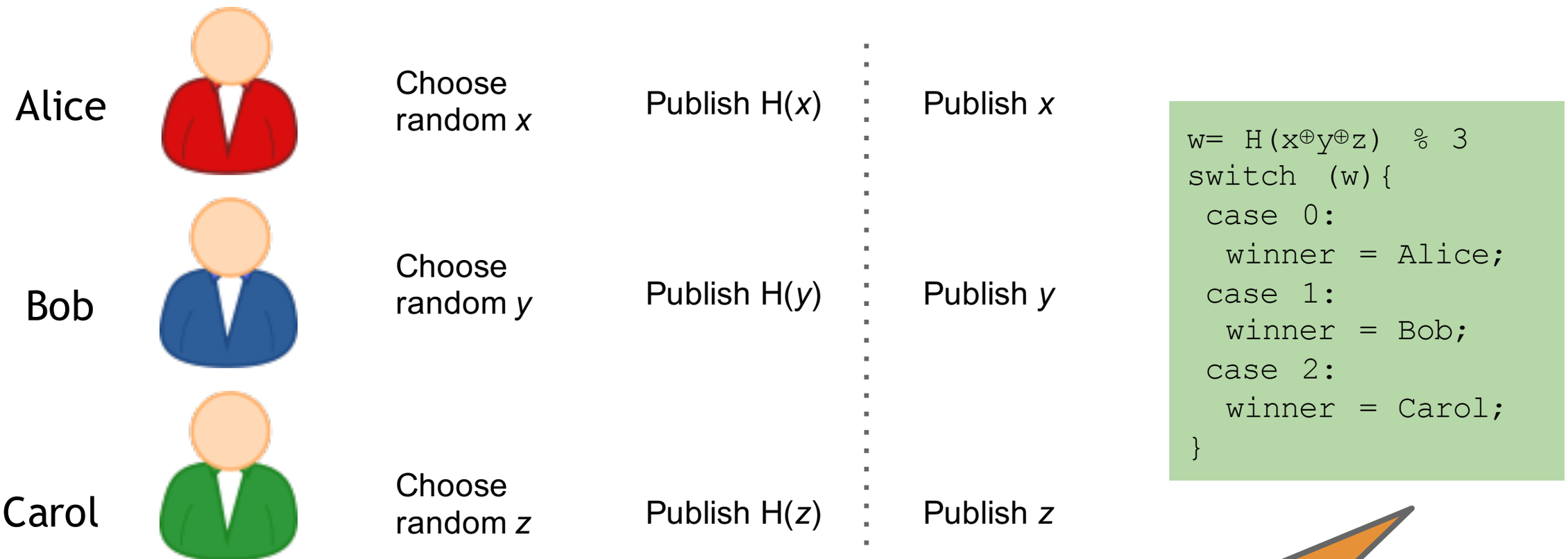
域名币

博彩

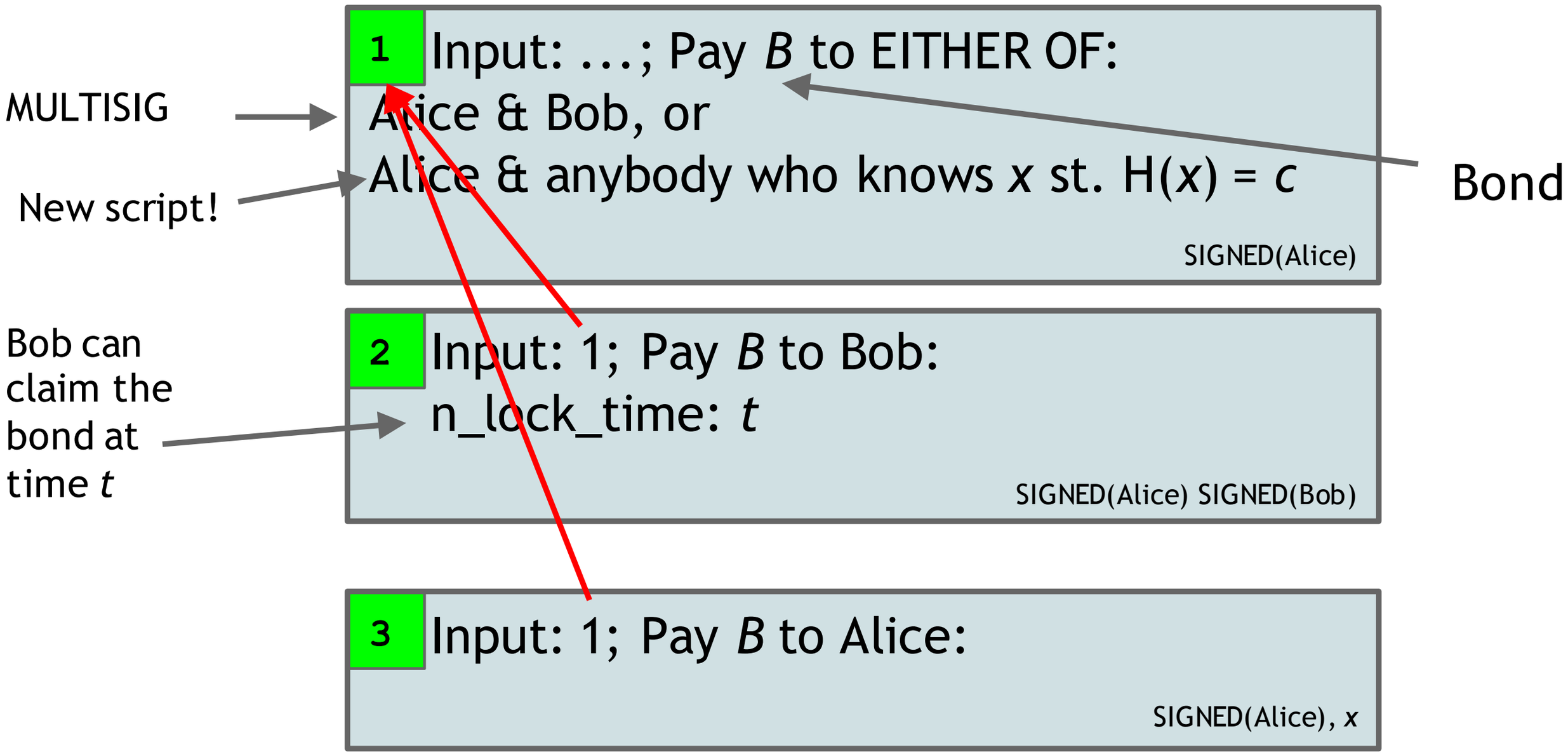

Wanna bet $5
Alice
Sure, I'll take heads!
Bob


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

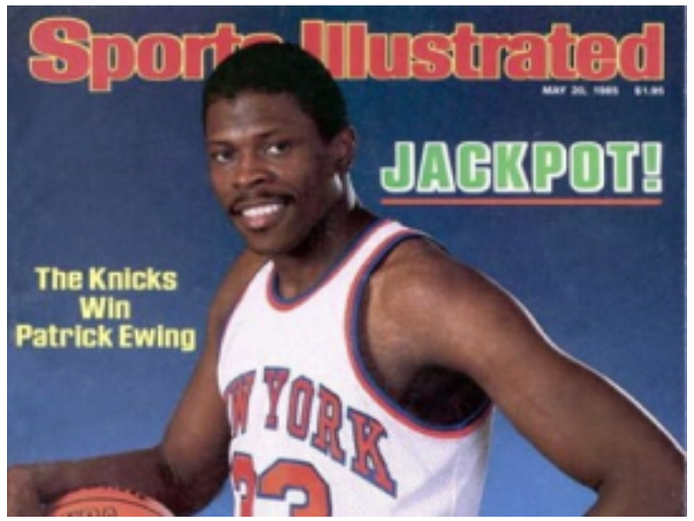
时间约束的在线博彩



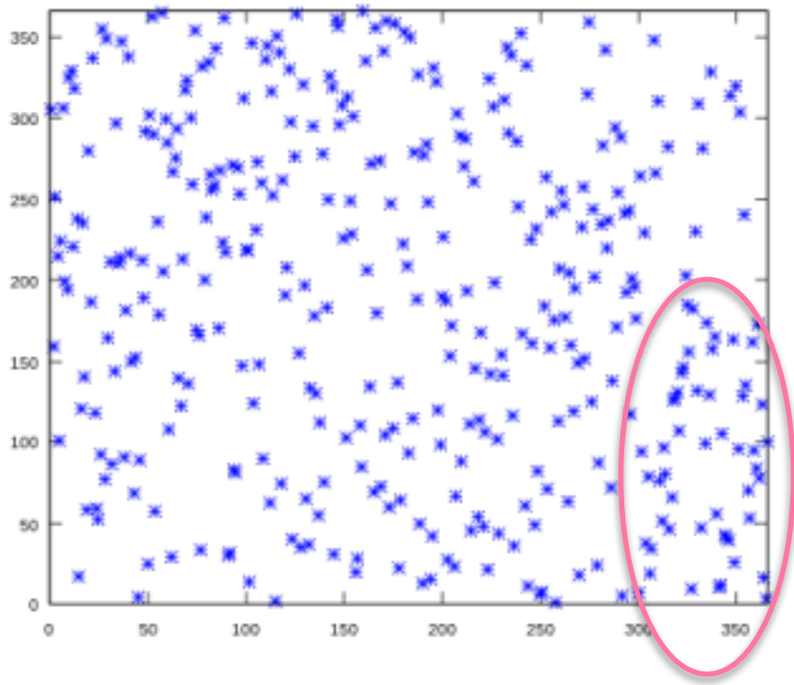
x revealed if Alice reclaims her bond

随机源

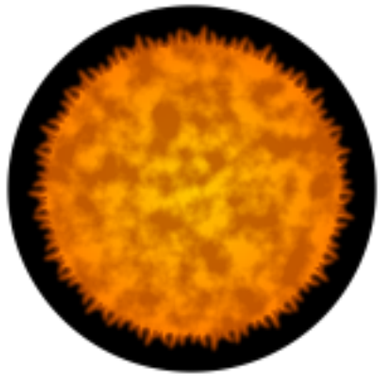

NBA
DRAFT
LOTTERY

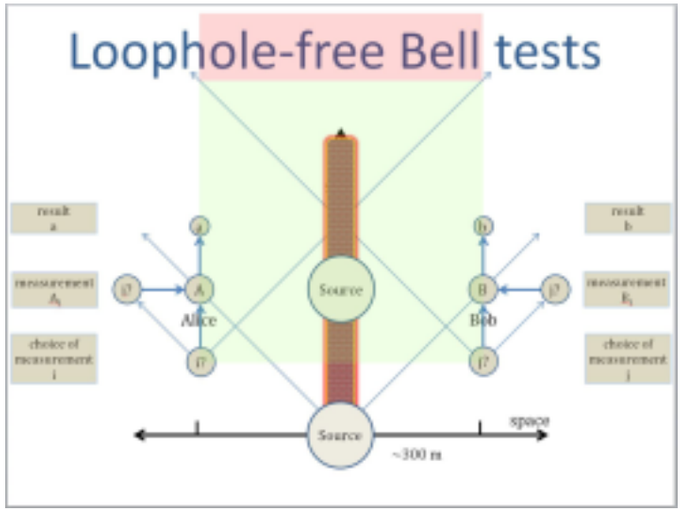

Sports Illustrated
JACKPOT!
The Knicks
Win
Patrick Ewing


Bent Corner

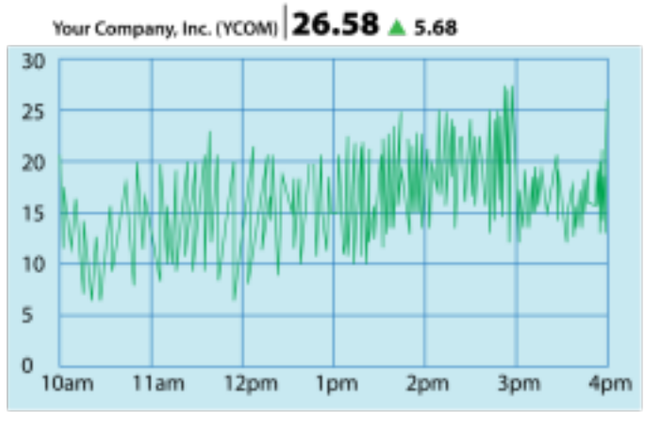

350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
350

随机源

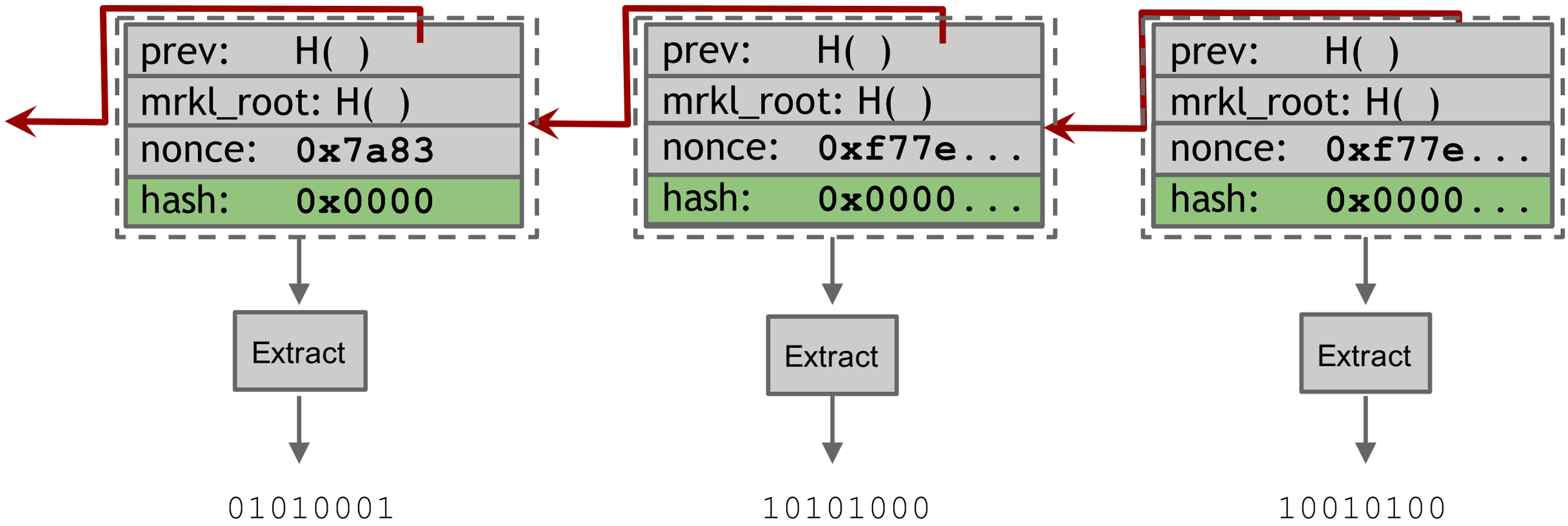



Loophole-free Bell tests
Source
Alice
Bob
Source
space
~300 m


BINGO


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

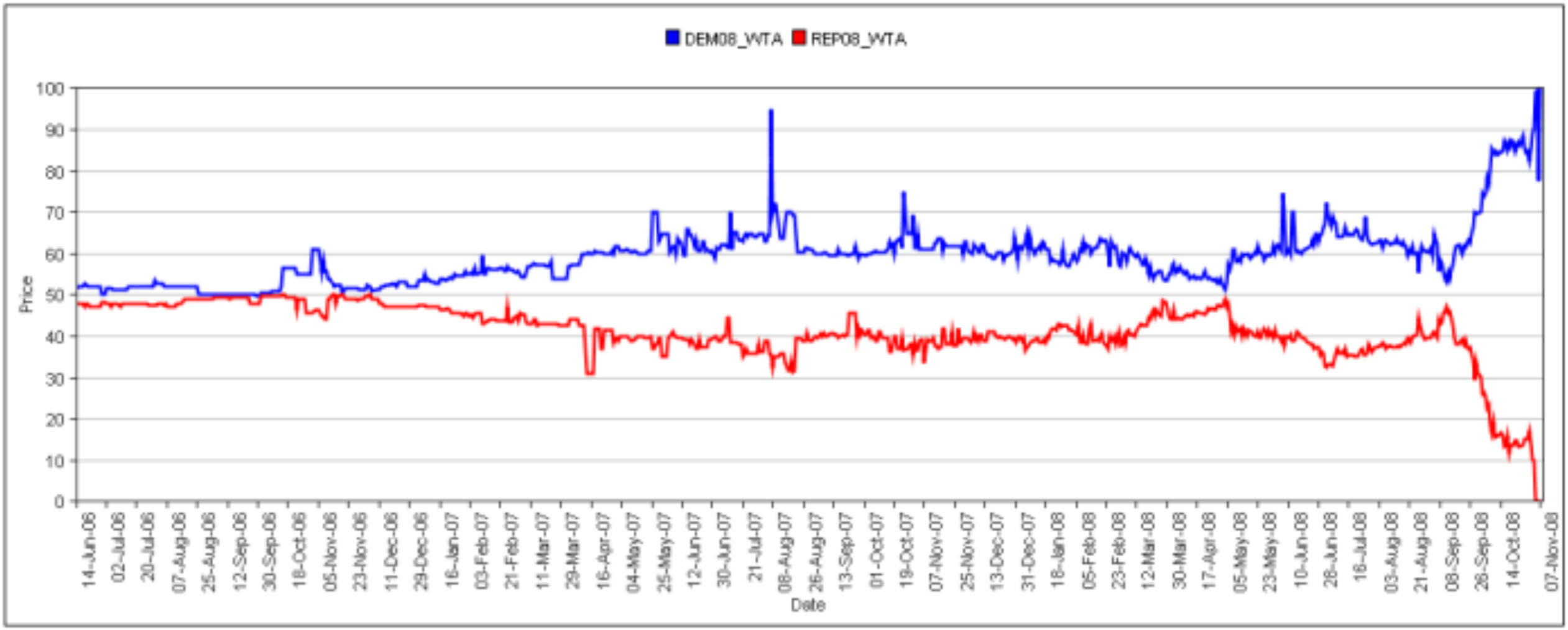
比特币作为随机源


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

Scottish independence referendum results to be for the independence

A month left

Sell at **0.50**

Buy at **1.40**

Scottish independence referendum results to be against the independence.

A month left

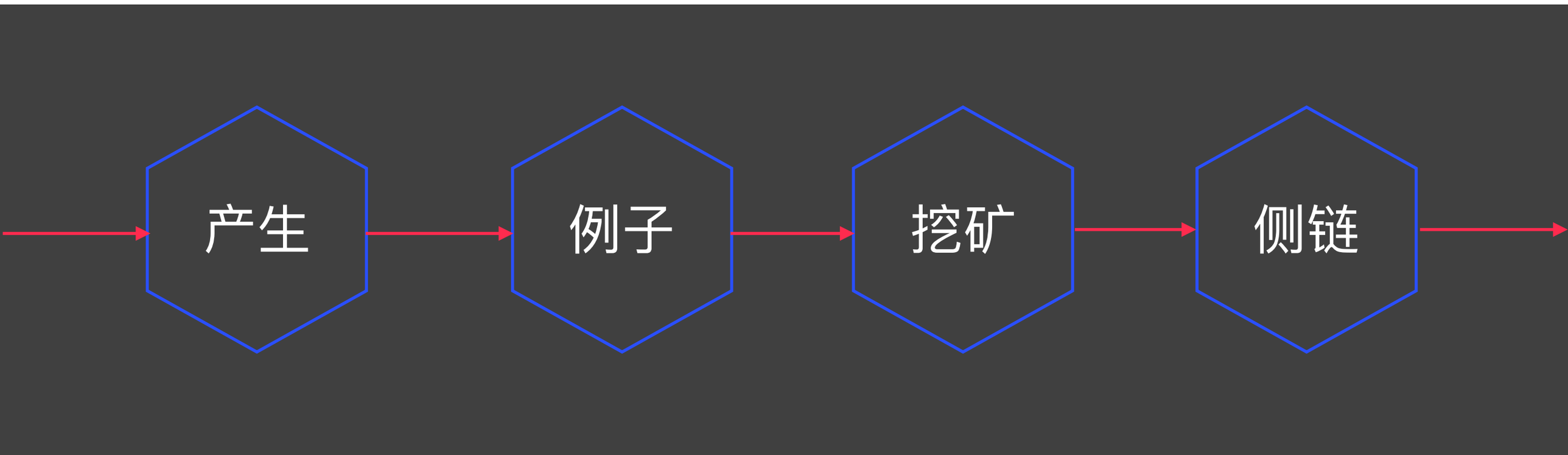
Sell at **8.60**

Buy at **9.50**

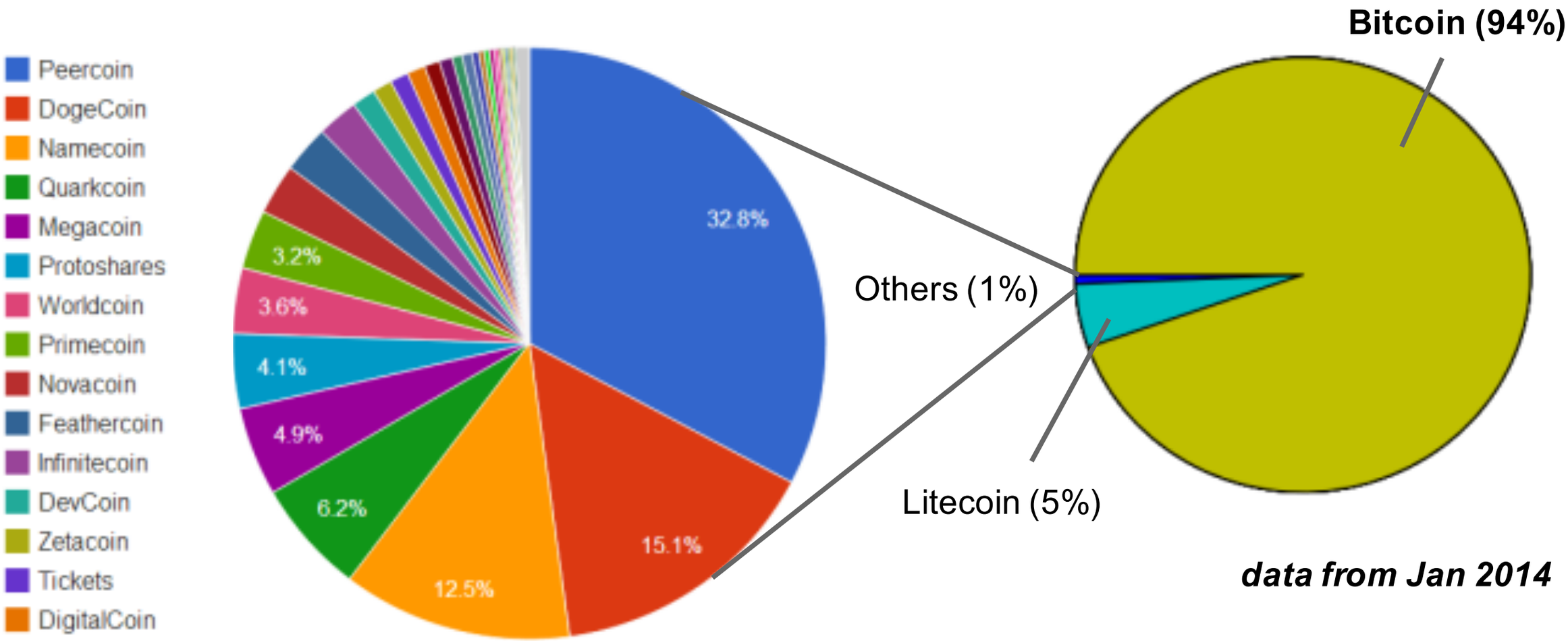
Orange?

Yellow?

其余代币



加密货币



data from Jan 2014

一些代币

为什么发行

吸引矿工

如何发行

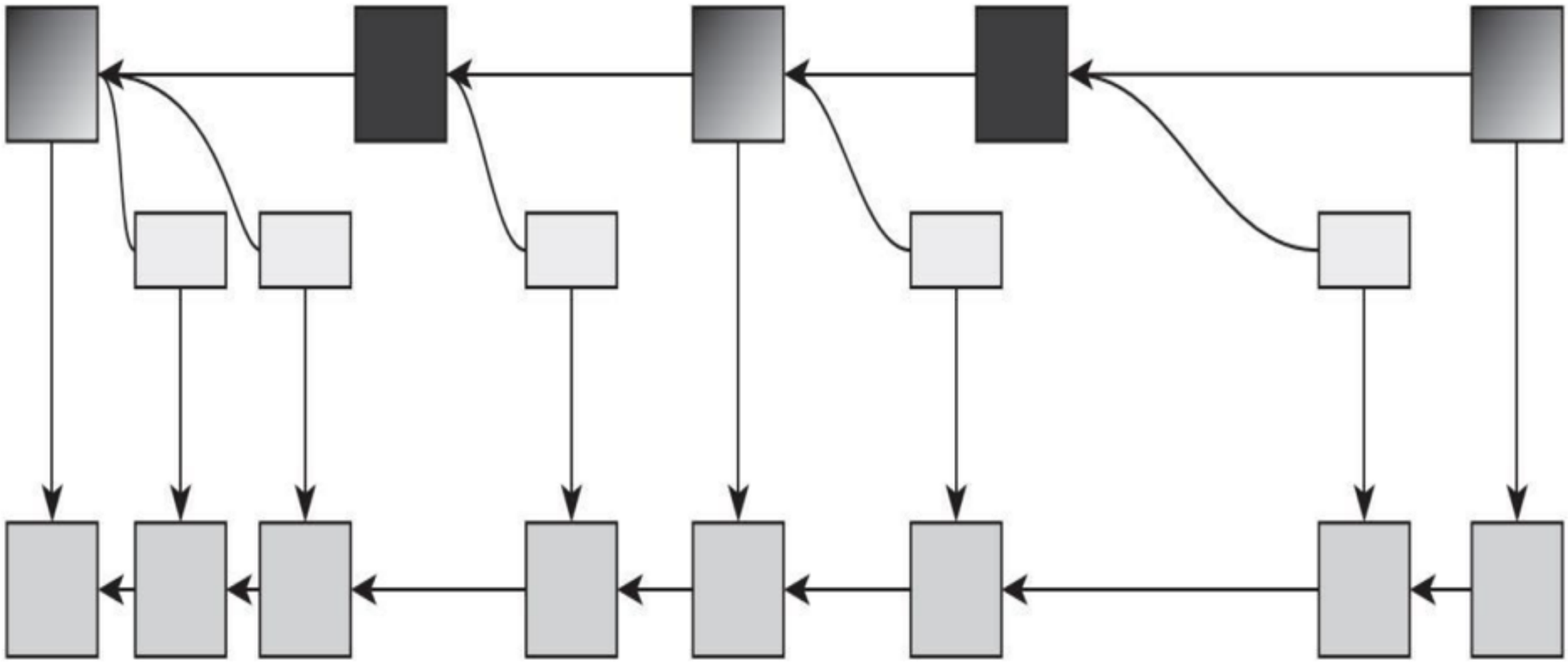
拉高出货

初始分配

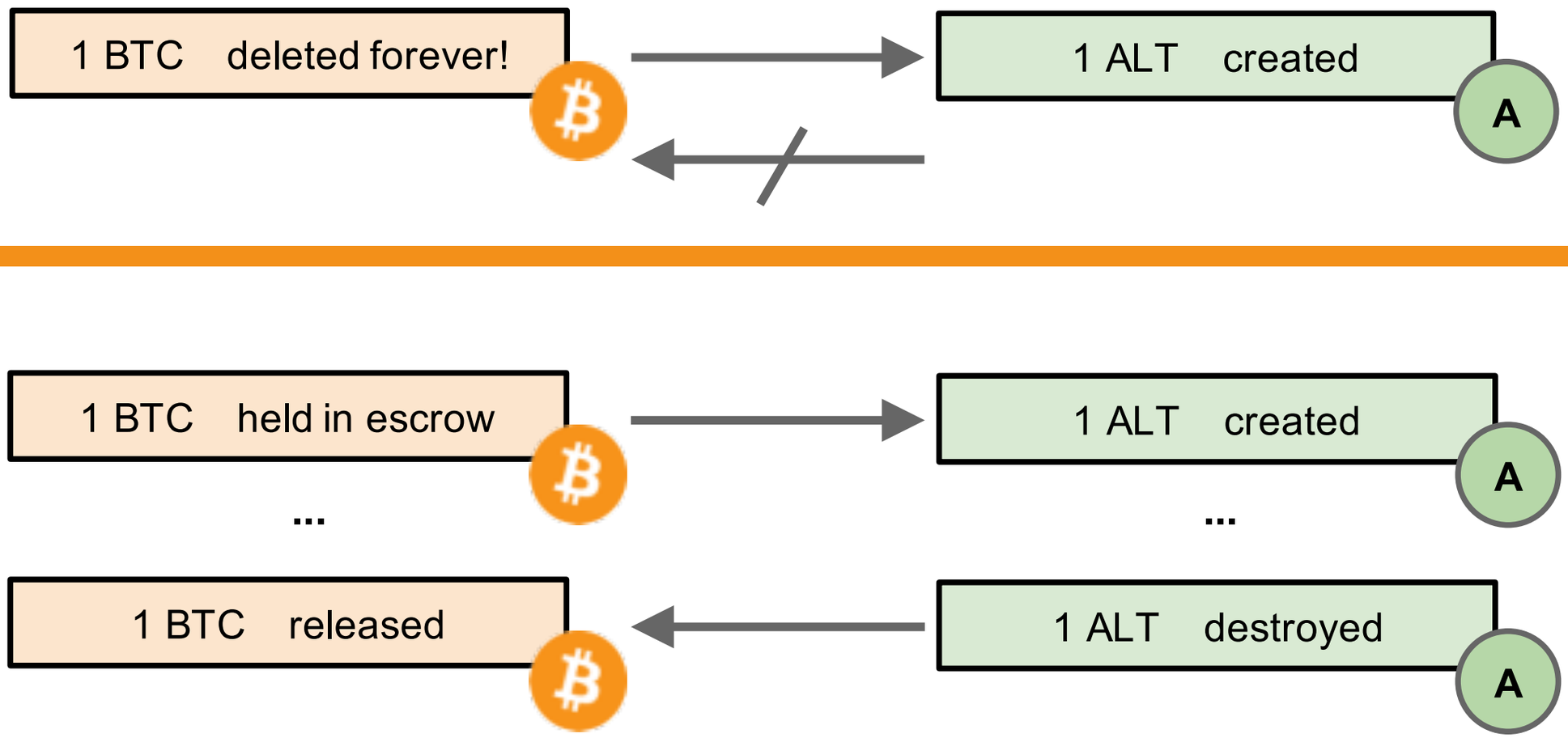
挖矿攻击

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

IPFS

IPFS is The Permanent Web

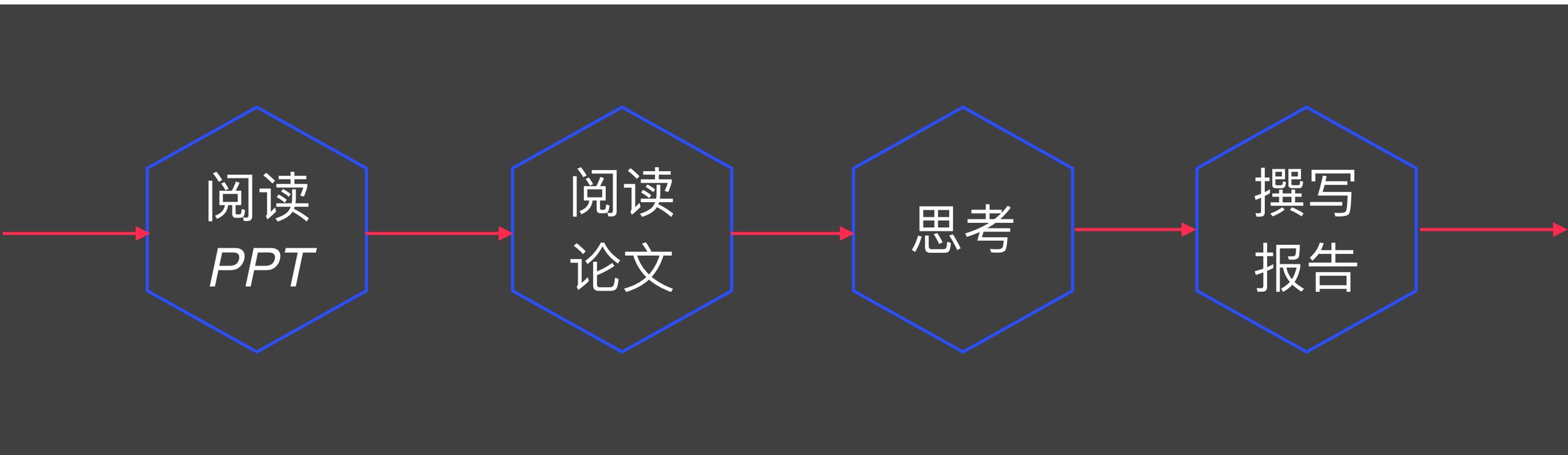
A new peer-to-peer hypermedia protocol

EOS

Decentralize Everything

HYPERLEDGER

课后作业



Homework

课后作业

要求阅读如下论文，写阅读报告

SmartPool: Practical Decentralized Pooled Mining

Loi Luu, *National University of Singapore;* Yaron Velner, *The Hebrew University of Jerusalem;*
Jason Teutsch, *TrueBit Foundation;* Prateek Saxena, *National University of Singapore*

https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/luu

In USENIX Security 2017.

1、论文概述

2、主要收获

3、存在疑问

4、所思所感

周六晚上12点前提交给助教

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io