

比特币 02



论文讲解

第四组

1 简介

2 原理

3 密钥和地址

4 钱包

- 教材
- 如何工作
- 概念定义
- 核心架构

- 买咖啡
- 交易构成
- 交易链
- 交易形式

- 公钥私钥
- 地址产生
- 靓号地址
- 纸钱包

- 钱包分类
- 非确定性
- 确定性
- HD、助记

1
区块

2
密码

3
共识

4
挖矿

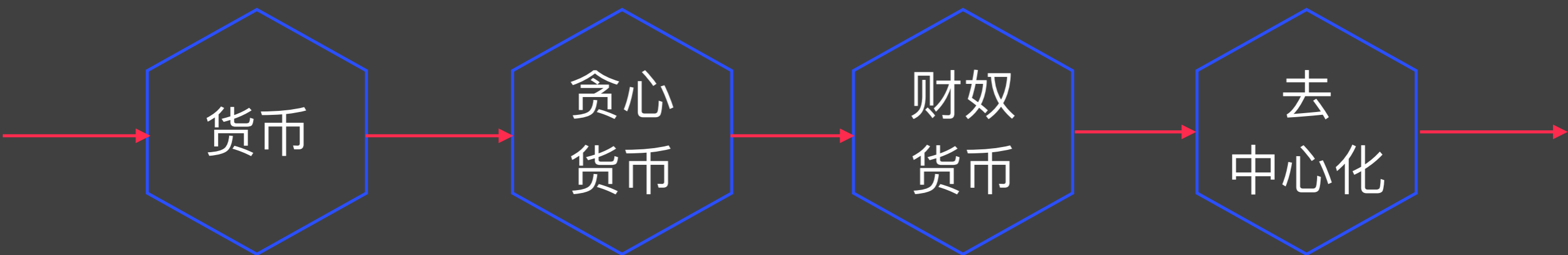
- Hash算法
- Hash指针
- 梅克尔树
- 区块结构

- 密码学
- 公钥密码学
- 公钥管理
- 数字签名

- P2P
- 分布共识
- 比特币共识
- 隐性共识

- 矿工任务
- 有效区块
- 激励机制
- 矿机矿池

加密货币



新版人民币 2015年版第5套 那些事...



钞票正面

钞票背面



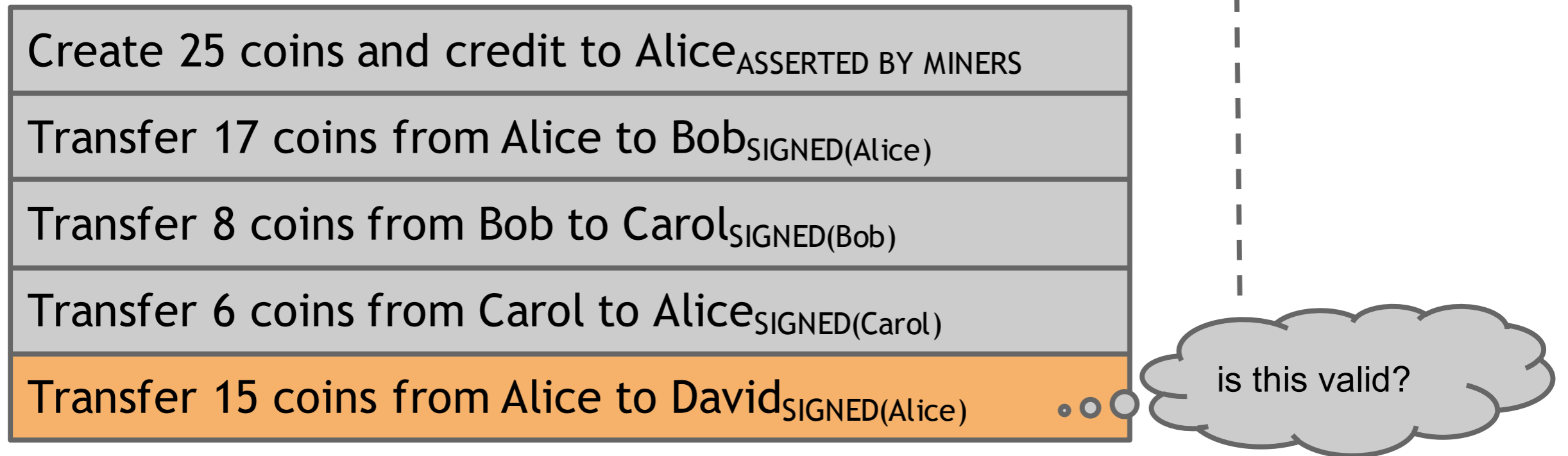
多一份金融了解 多一份财富保障

2015年版第5套人民币100元纸币在保持2005年版第五套人民币100元纸币规格、正背面主图案、主色调、“中国人民银行”行名、国徽、盲文和汉语拼音行名、民族文字等不变的前提下，对部分图案做了调整，对整体防伪性能进行了提升。

- 1 光变镂空开窗安全线**
位于票面正面右侧。垂直票面观察，安全线呈品红色；与票面成一定角度观察，安全线呈绿色；透光观察，票面安全线中正反交替排列的镂空文字“¥100”。
- 2 雕刻凹印**
票面正面毛泽东头像、国徽、“中国人民银行”行名、右上角面额数字、盲文及背面人民大会堂等均采用雕刻凹印印刷，用手指触摸有明显的凹凸感。
- 3 胶印对印图案**
票面正下方和背面右下方均有面额数字“100”的局部图案。透光观察，正背面图案组成一个完整的图案数字“100”。
- 4 光彩光变数字**
位于票面正面中部。垂直票面观察，数字以金色为主；平视观察，数字以绿色为主。随着观察角度的改变，数字颜色在金色与绿色之间交替变化，并可见到一条亮光带上下滚动。
- 5 白水印**
位于票面正面横号码下方。透光观察，可以看到透光很强的水印面额数字“100”。
- 6 人像水印**
位于票面正面左侧空白处。透光观察，可见毛泽东头像。
- 7 横竖双号码**
票面正面左下方采用横号码，其冠字和前两位数字为暗红色，后六位数字为黑色；右侧竖号码为蓝色。



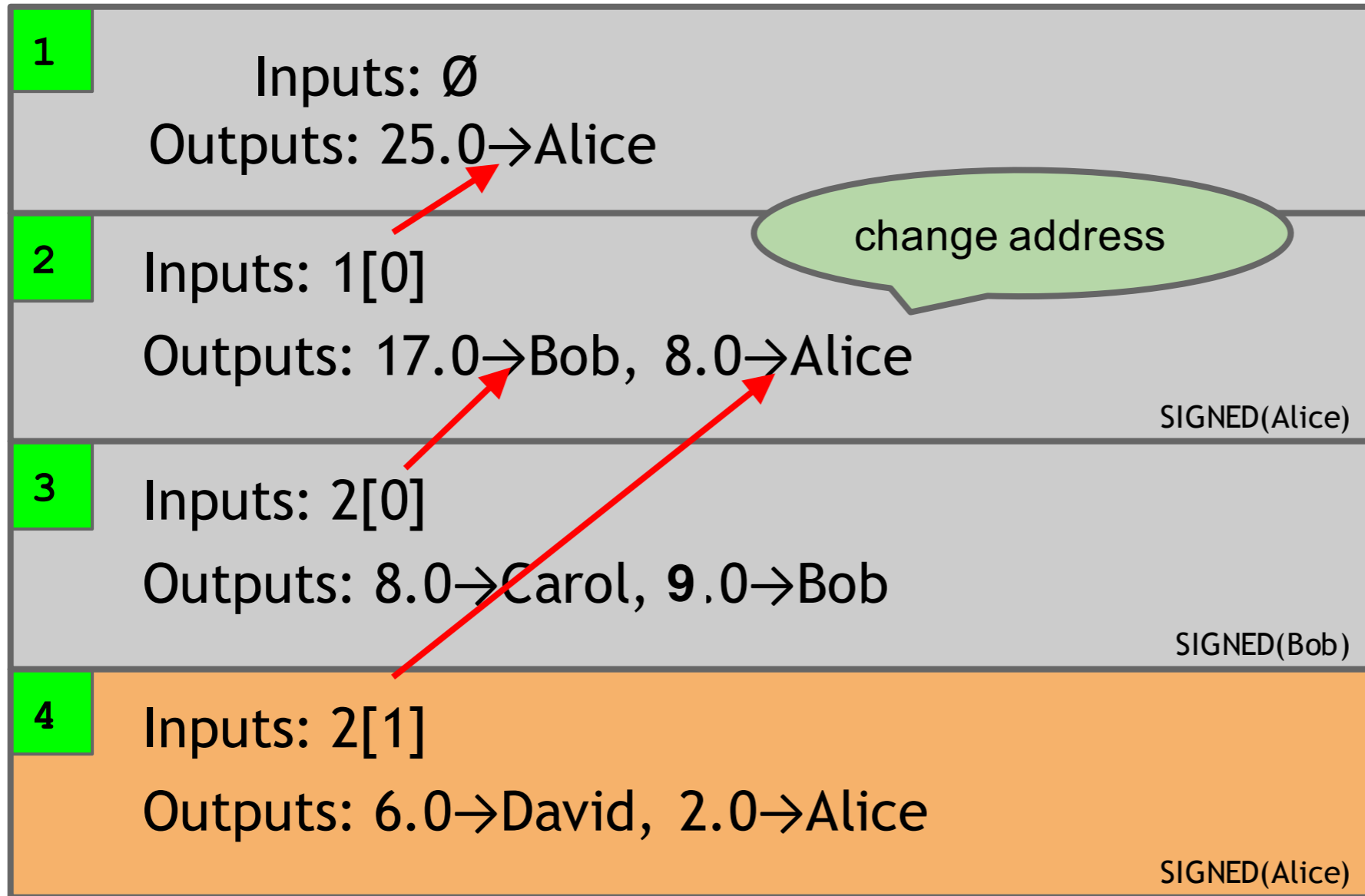
时间



一个块包含一个交易

交易验证需要扫描以前所有的块

时间



we implement this with hash pointers

finite scan to check for validity

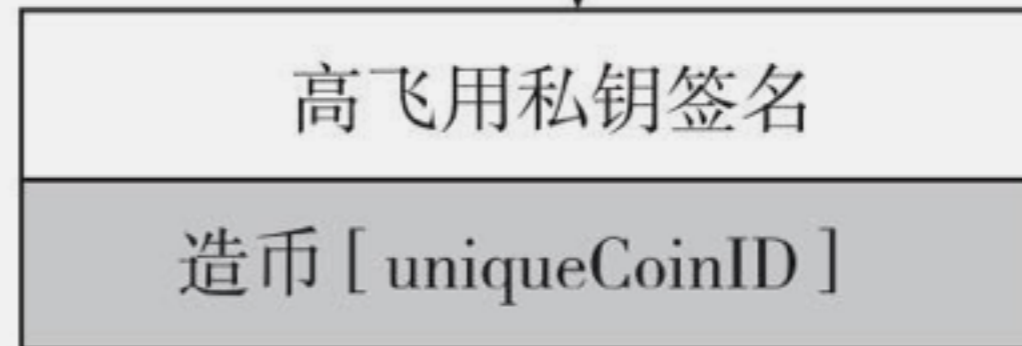
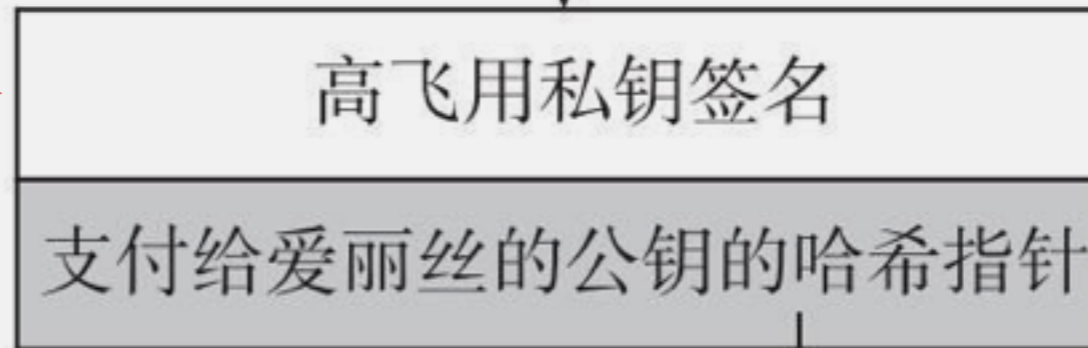
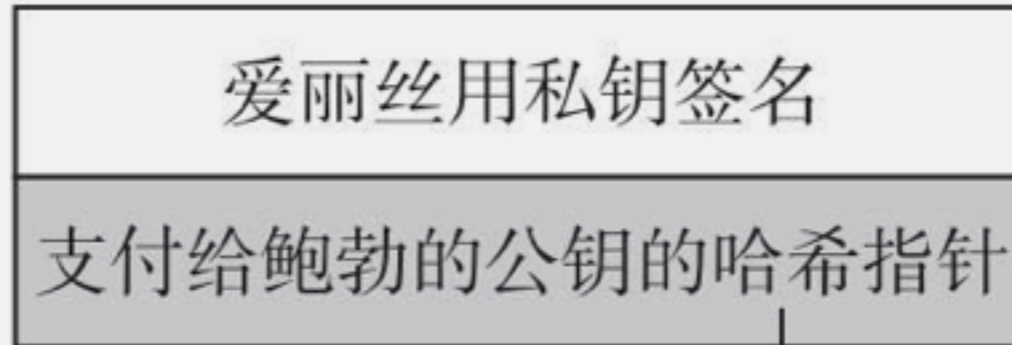
is this valid?

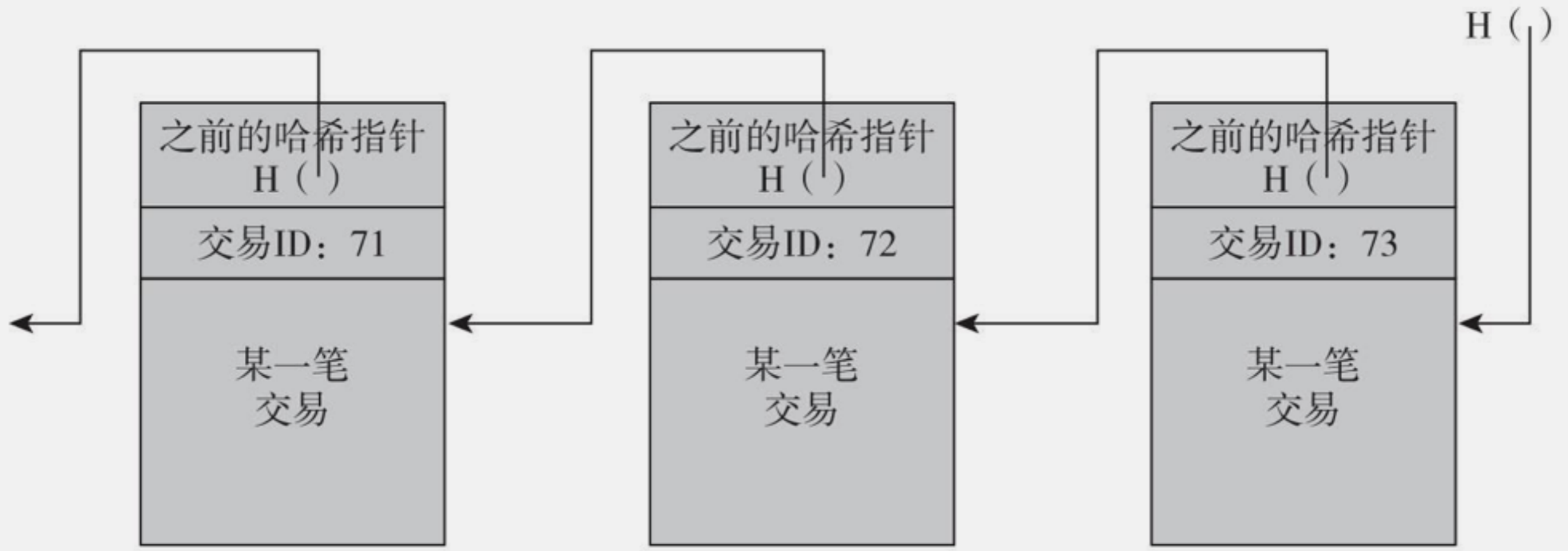
一个块包含一个交易

交易验证需要扫描以前所有的相关块

爱丽丝支付给
查克

双重花费





需要中心结构支持

为什么要去中心化

- 谁维护交易账本?
- 谁有权限验证交易的有效性?
- 谁创造新的比特币?

- 谁决定系统如何改变规则?
- 比特币如何获得交易价格

技术

激励

用户: 对等网络 / 矿工 挖矿 / 开发人员: 软件更新

窃取比特币

拒绝服务攻击

双重支付攻击

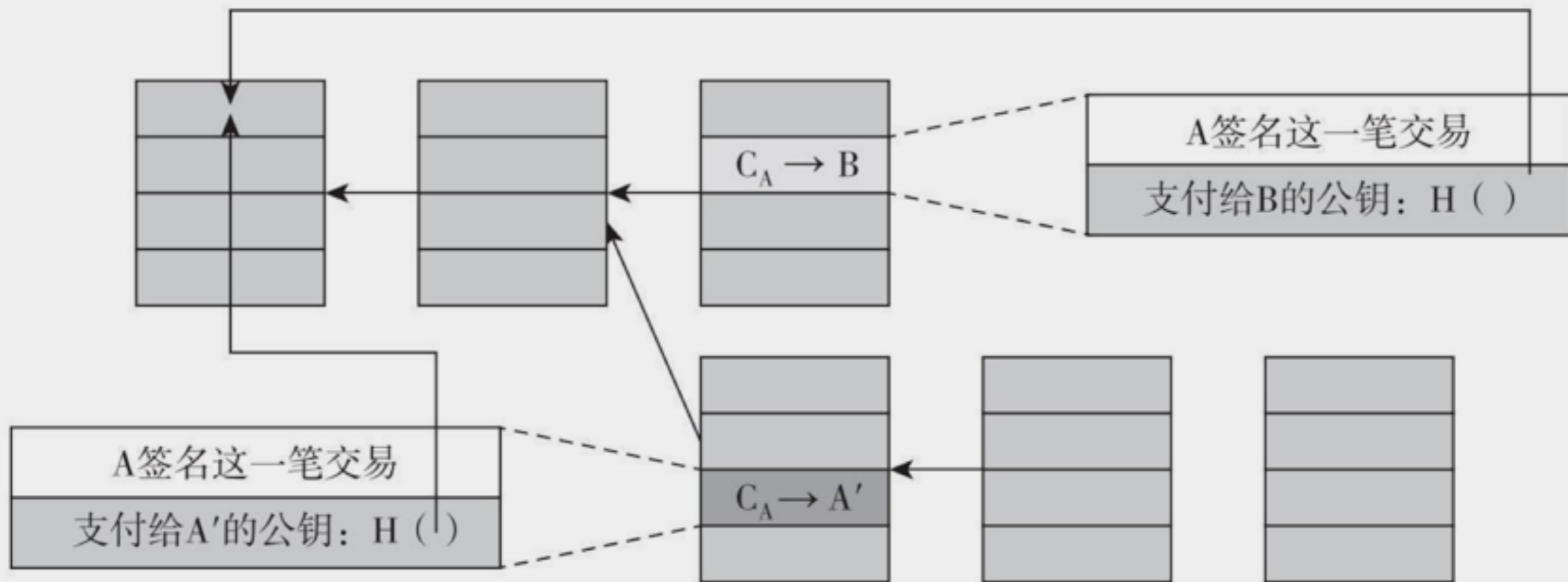


图2.2 双重支付攻击

注：爱丽丝创建了两笔交易：一笔是她付给鲍勃比特币的交易，另一笔是她将这笔比特币重复支付到她控制的另一个地址。因为这两笔交易用相同的比特币支付，所以只有一笔会被放进区块链。图中的箭头表示一个区块链接到前一个区块的指针，通过在前一个区块自己的内容中包含了一个哈希值进行了扩展。 C_A 代表爱丽丝拥有的币。

双重支付攻击防止：等待多次确认

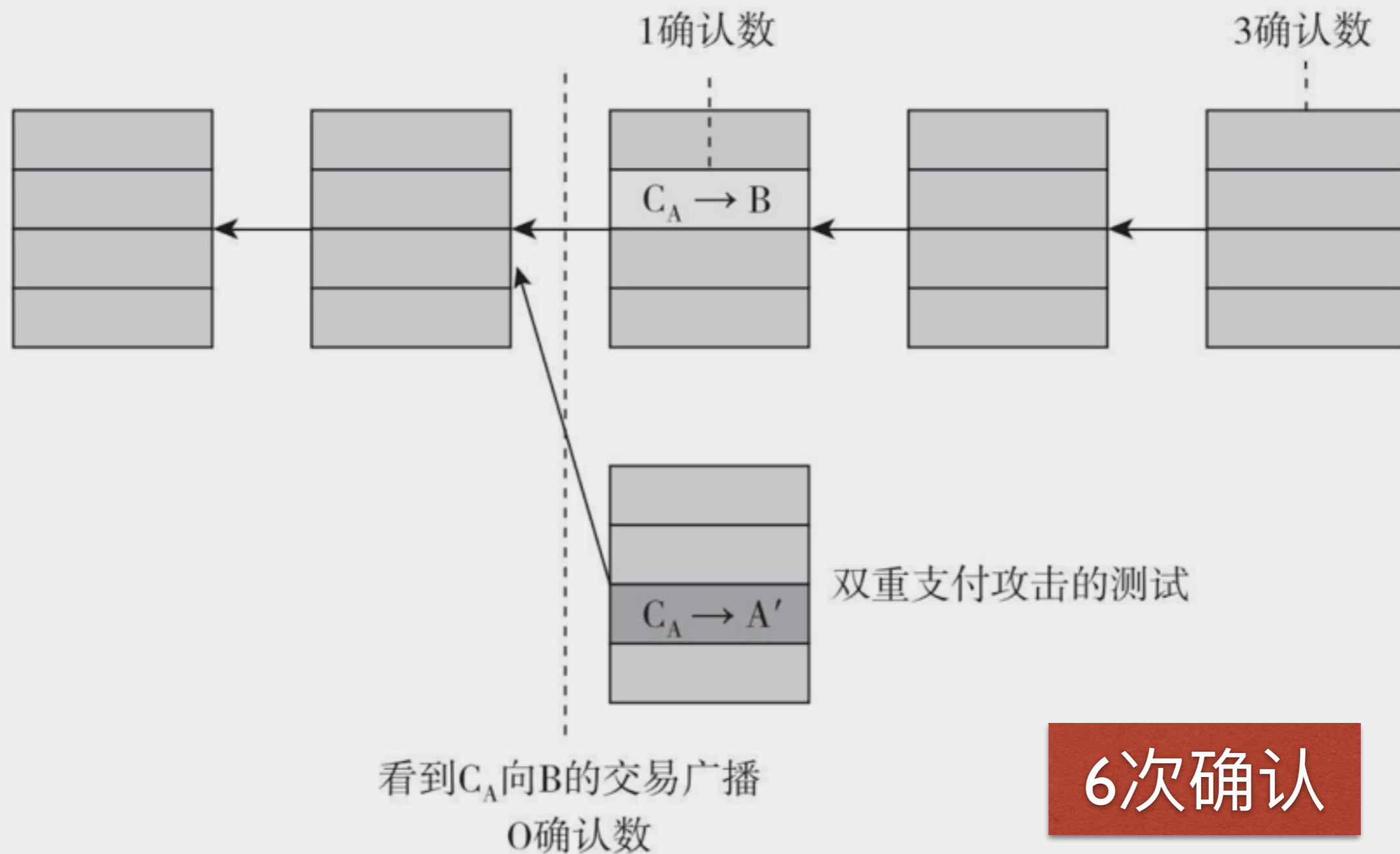
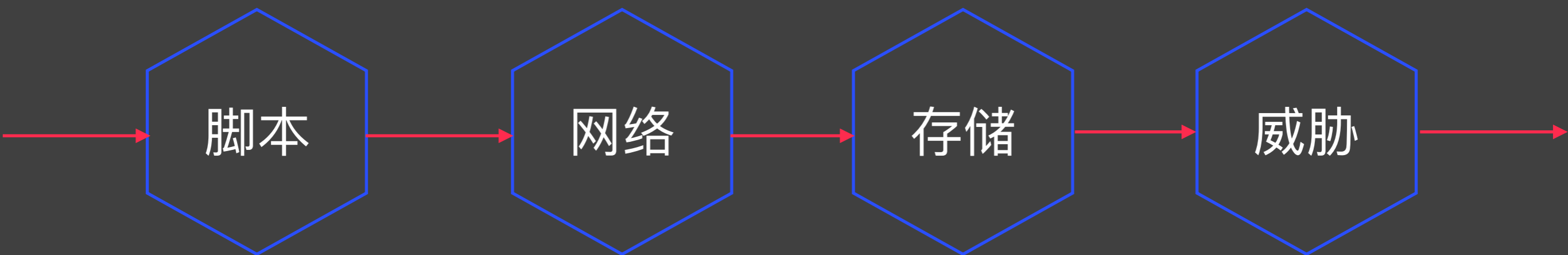


图2.3 从鲍勃立场来看双重支付

注：这是一个从商家鲍勃的立场来看爱丽丝做的双重支付尝试。为了保护自己免受双重支付攻击，鲍勃应当等爱丽丝向他支付的交易被区块链包含进去，并且多等几次确认。

运行机制



```

OP_DUP
OP_HASH160
69e02e18...
OP_EQUALVERIFY
OP_CHECKSIG

```

图3.4 P2PH脚本范例

```

<sig>
<pubKey>
-----
OP_DUP
OP_HASH160
<pubKeyHash?>
OP_EQUALVERIFY
OP_CHECKSIG

```

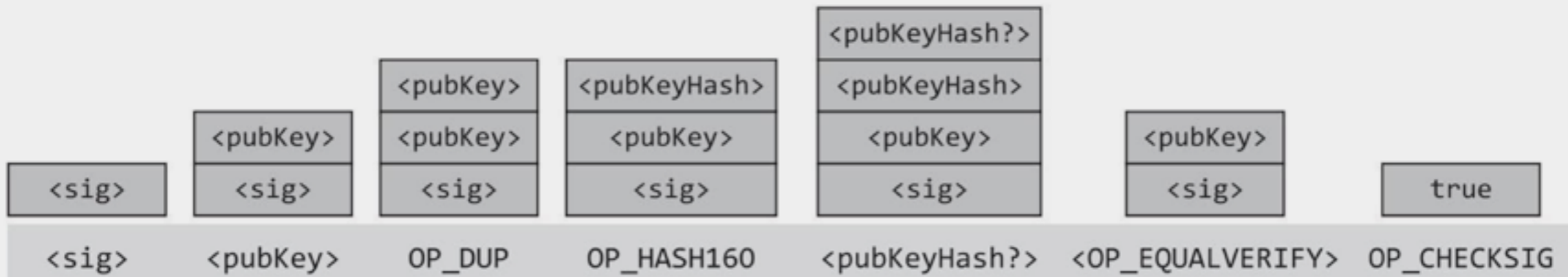


图3.6 比特币脚本的执行堆栈状态图

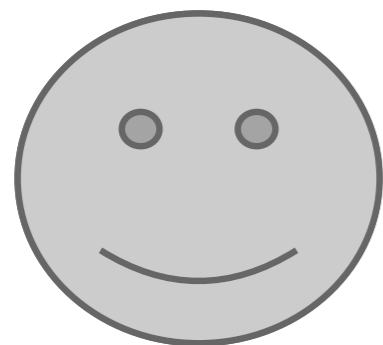
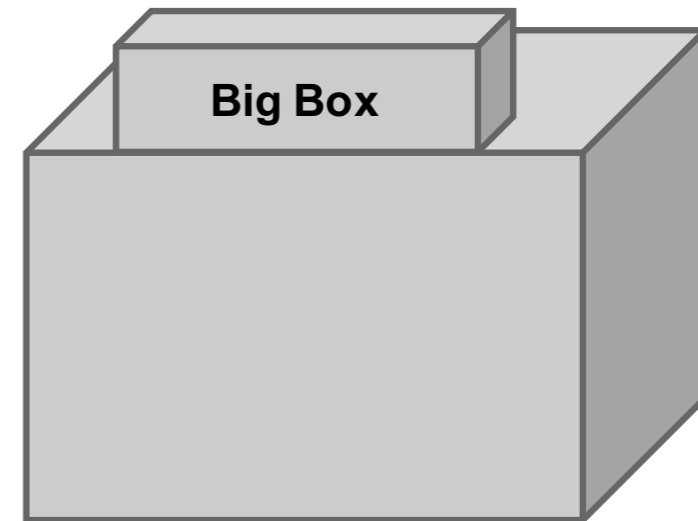
注：图中底部列出了相对应的指令：尖括号里的是数据指令，以OP开头的是工作码指令，指令上方对应的是指令执行之后的堆栈状态。



I'm ready to pay for my purchases!



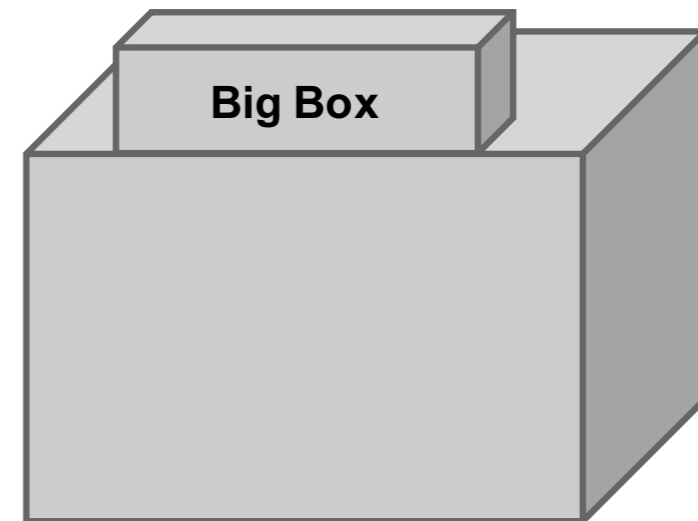
Cool! Well we're using MULTISIG now, so include a script requiring 2 of our 3 account managers to approve. Don't get any of those details wrong. Thanks for shopping at Big Box!



I'm ready to pay for my purchases!



Great! Here's our address: 0x3454




```
{
  "hash": "5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver": 1,
  "vin_sz": 2,
  "vout_sz": 1,
  "lock_time": 0,
  "size": 404,
  "in": [
    {
      "prev_out": {
        "hash": "3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
        "n": 0
      },
      "scriptSig": "30440..."
    },
    {
      "prev_out": {
        "hash": "7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
        "n": 0
      },
      "scriptSig": "3f3a4..."
    }
  ],
  "out": [
    {
      "value": "10.12287097",
      "scriptPubKey": "OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e
        OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```

元数据

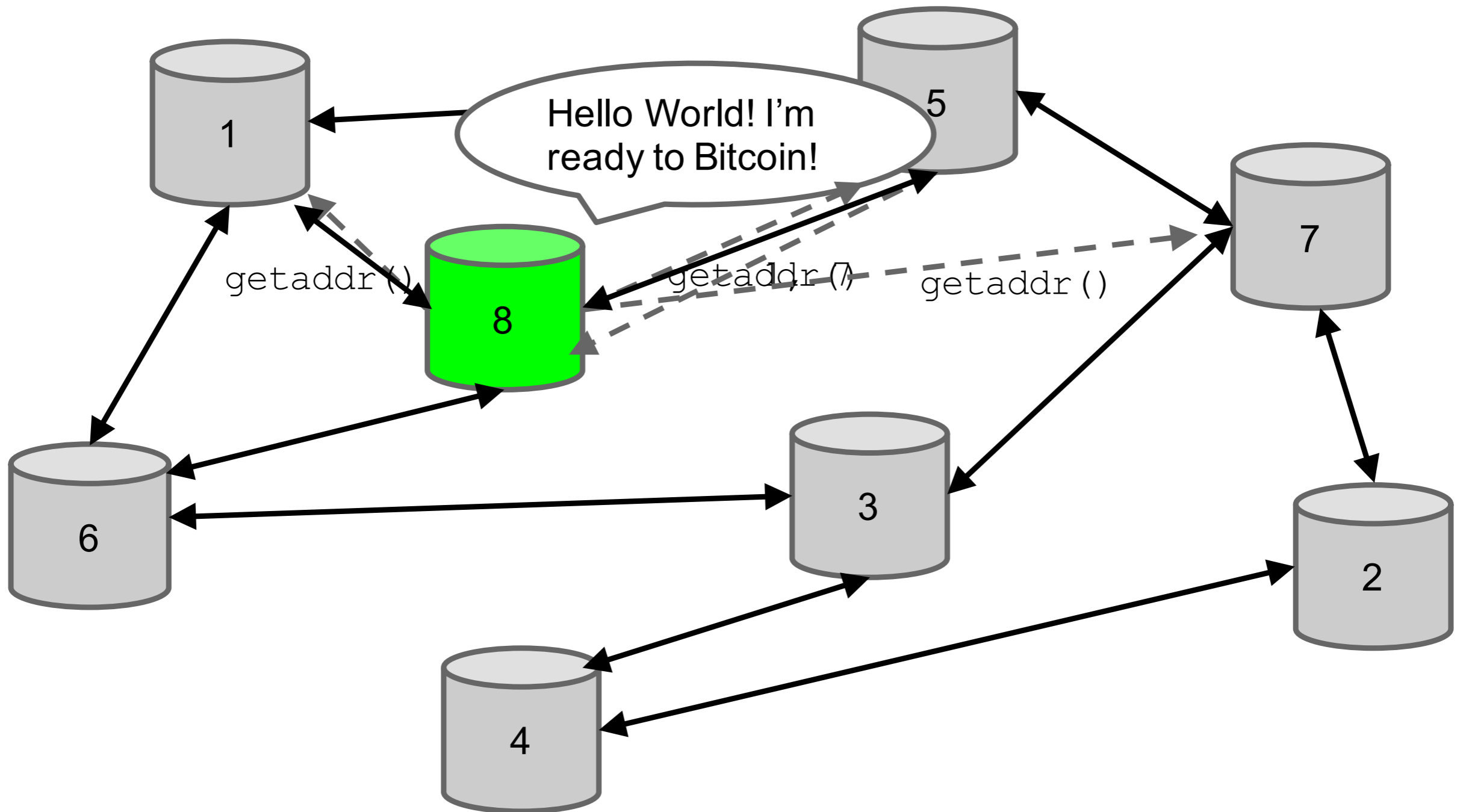
输入

输出

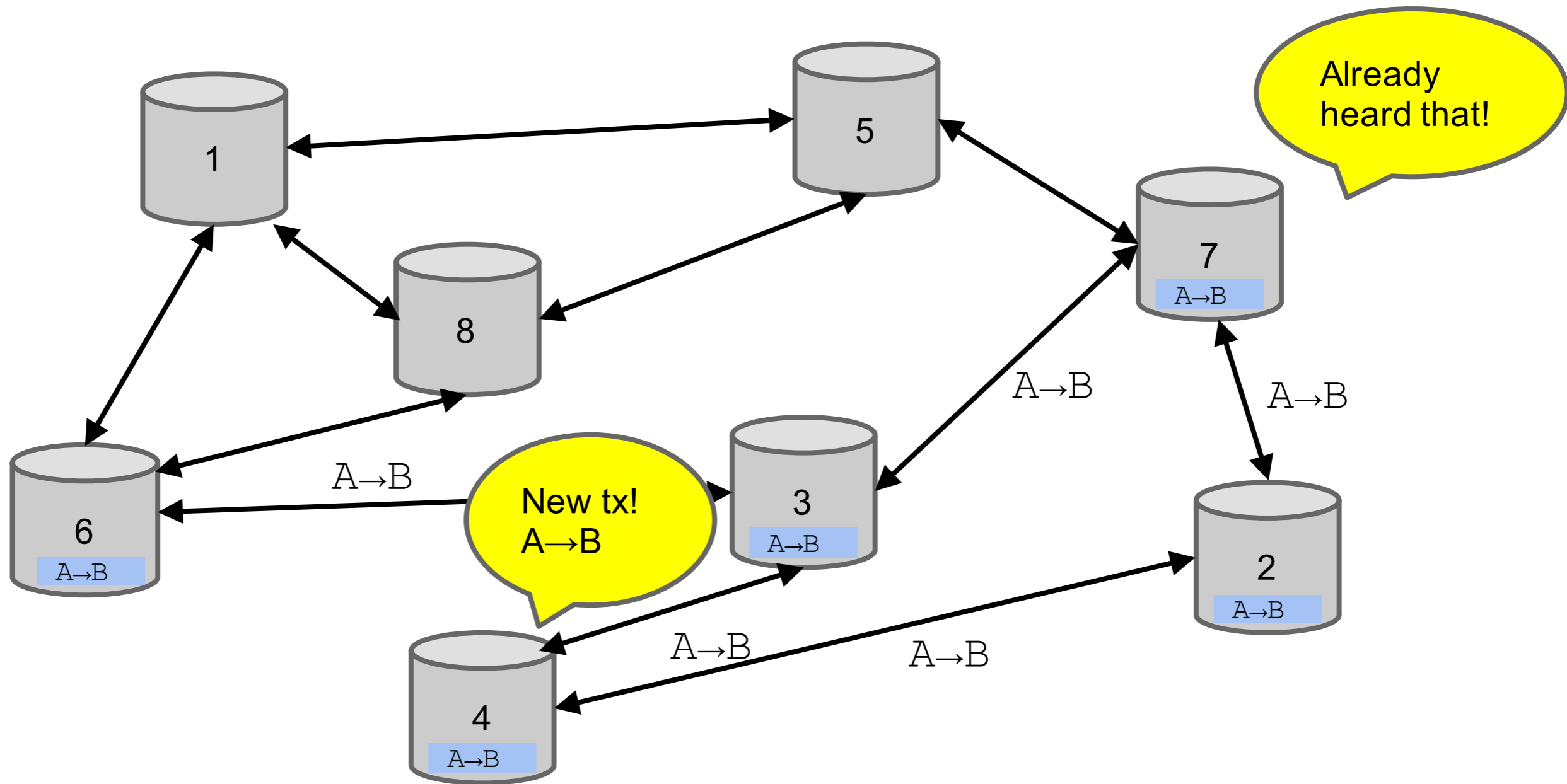
图3.3 一个真实的比特币交易程序段

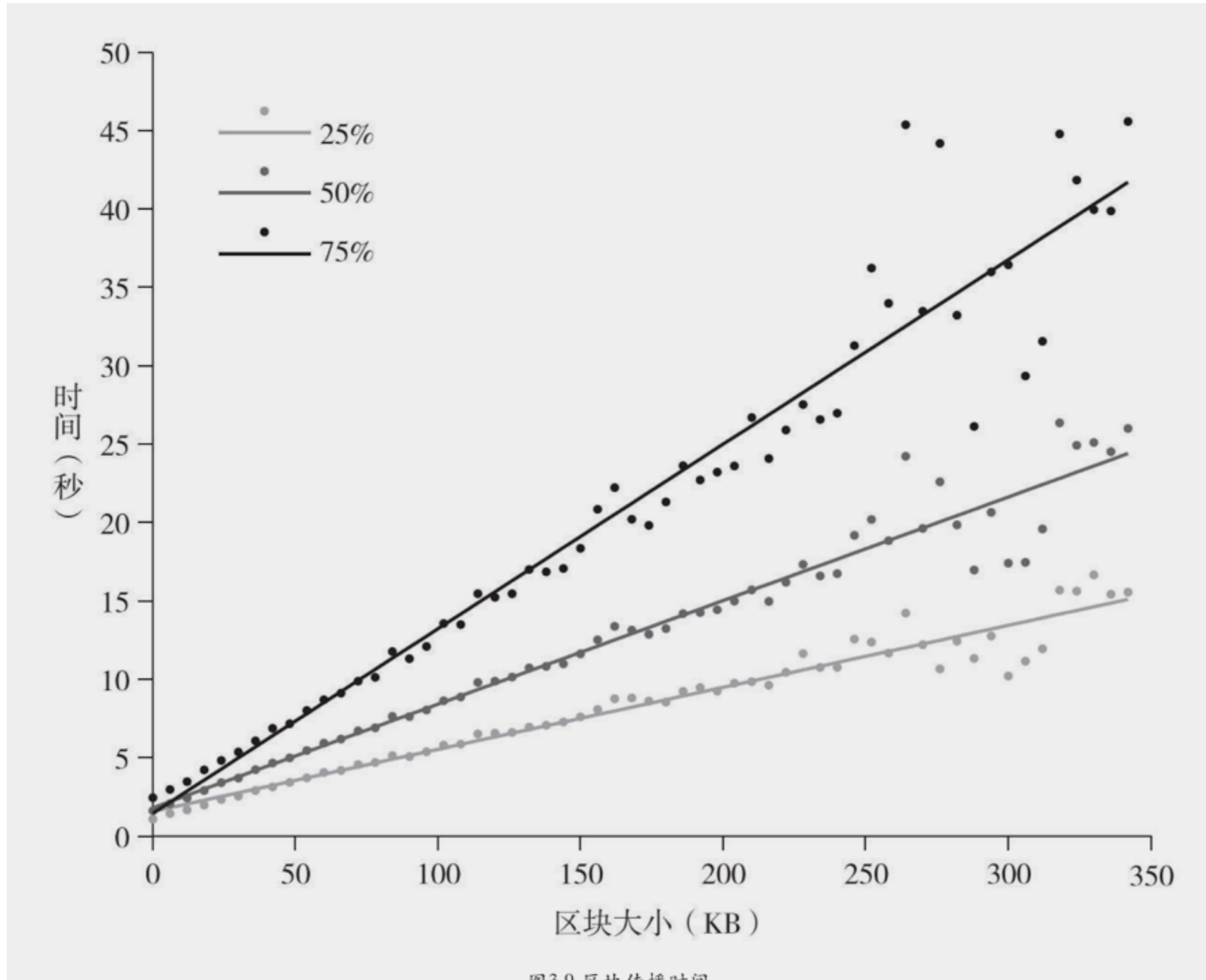
```
"in":[
  {
    "prev_out":{
      "hash":"000000.....0000000",
      "n":4294967295
    },
    "coinbase":"..."
  },
  [
    "out":[
      {
        "value":"25.03371419",
        "scriptPubKey":"OPDUP OPHASH160 ... "
      }
    ]
  ]
]
```

图3.8 币基交易



比特币网络交易消息传播





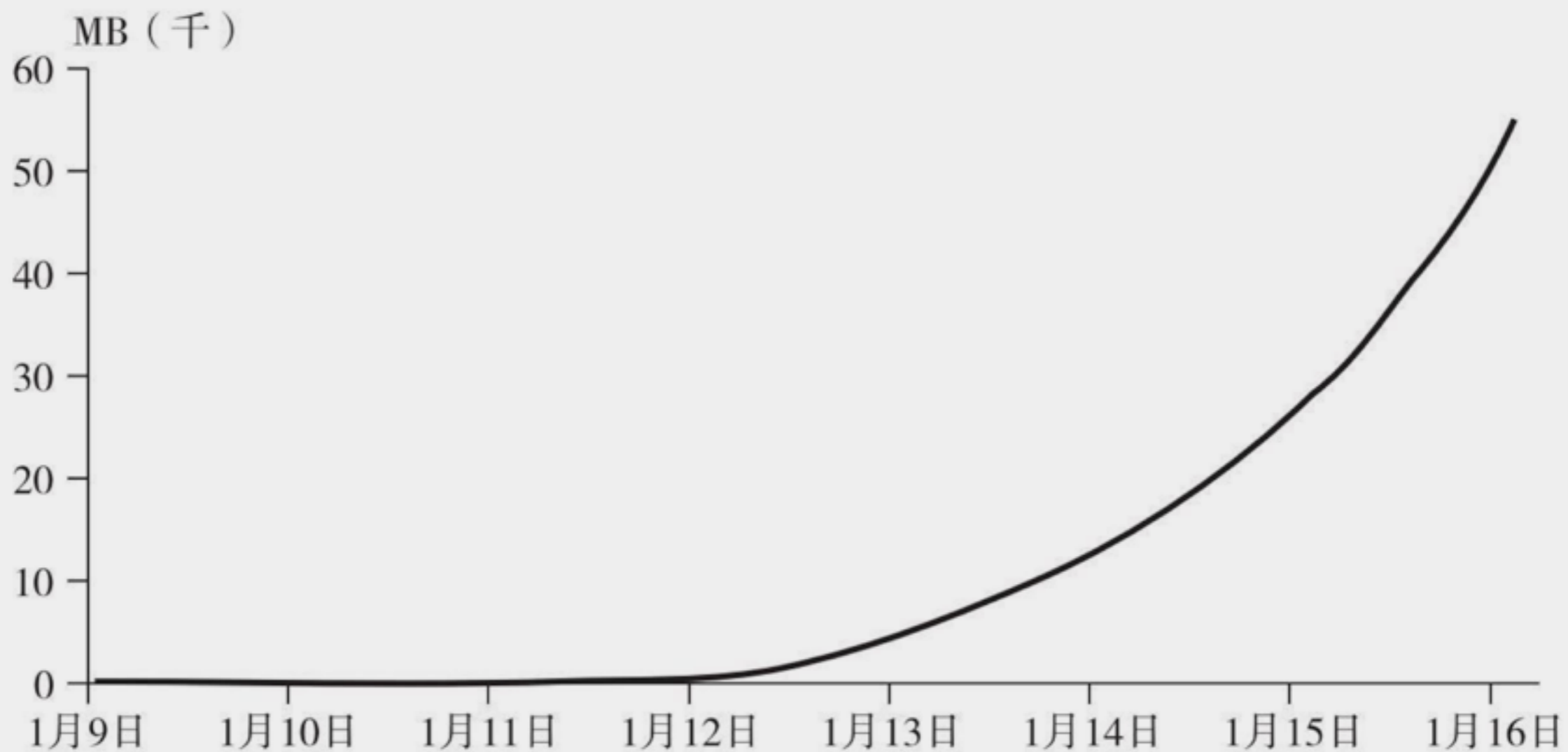
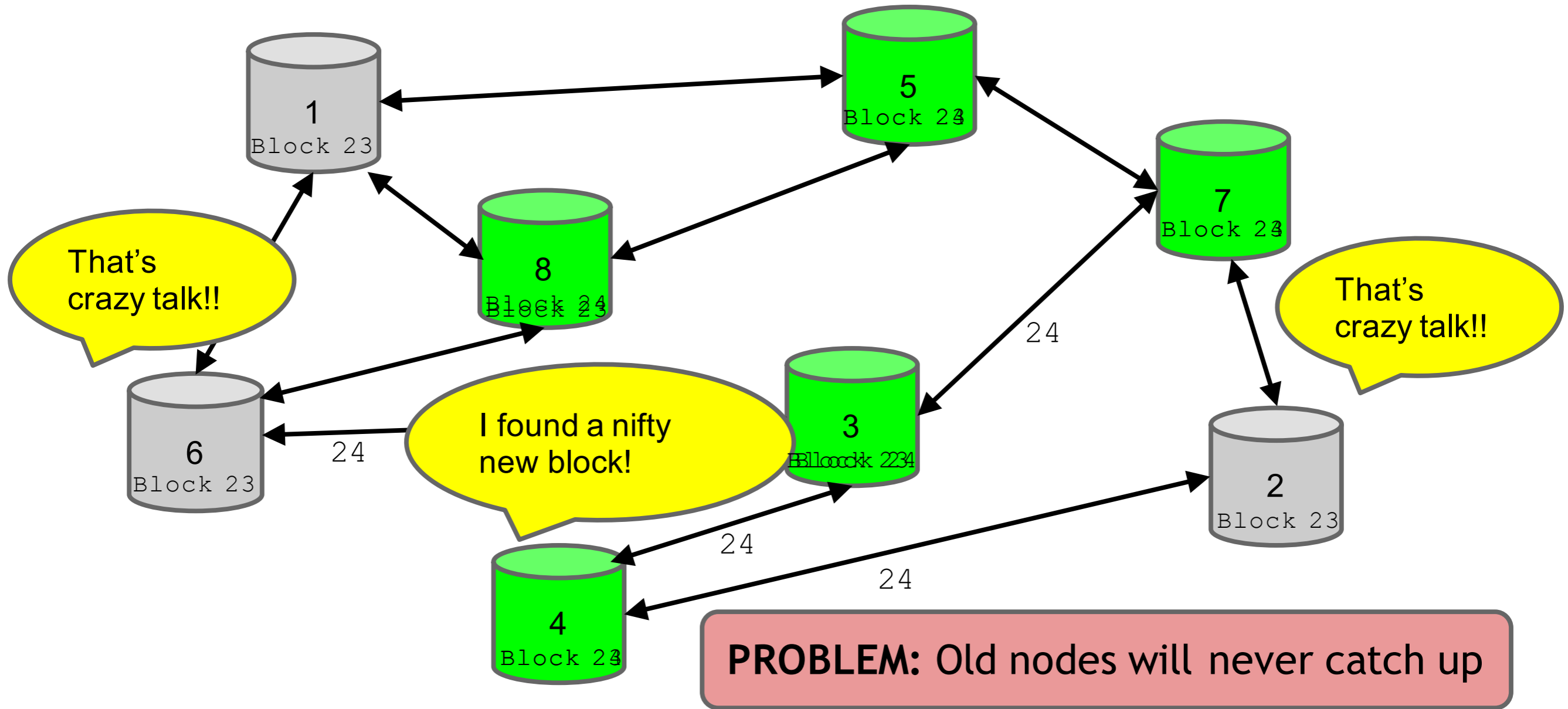


图3.10 区块链的大小

注：全节点必须保持整个区块链，在2015年年底，区块链大小在50GB以上。



硬 vs. 软

Hot storage



online

hot secret key(s)

cold address(es)

Cold storage



offline

payments





Charles Ponzi



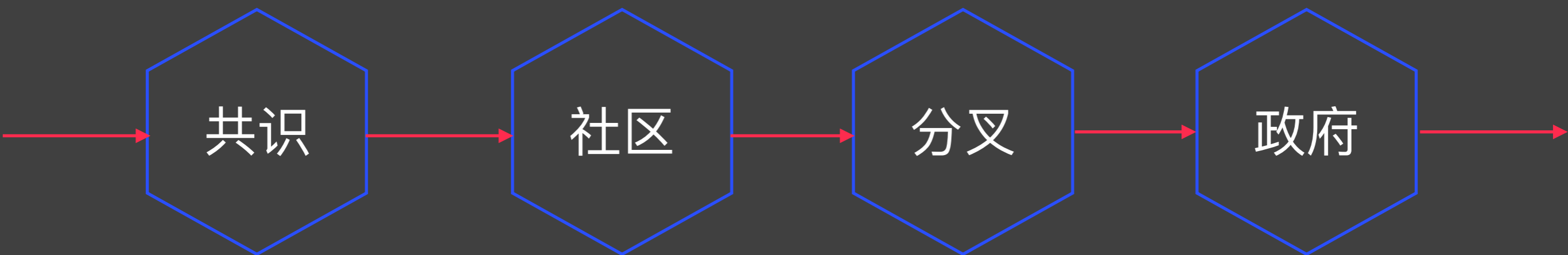


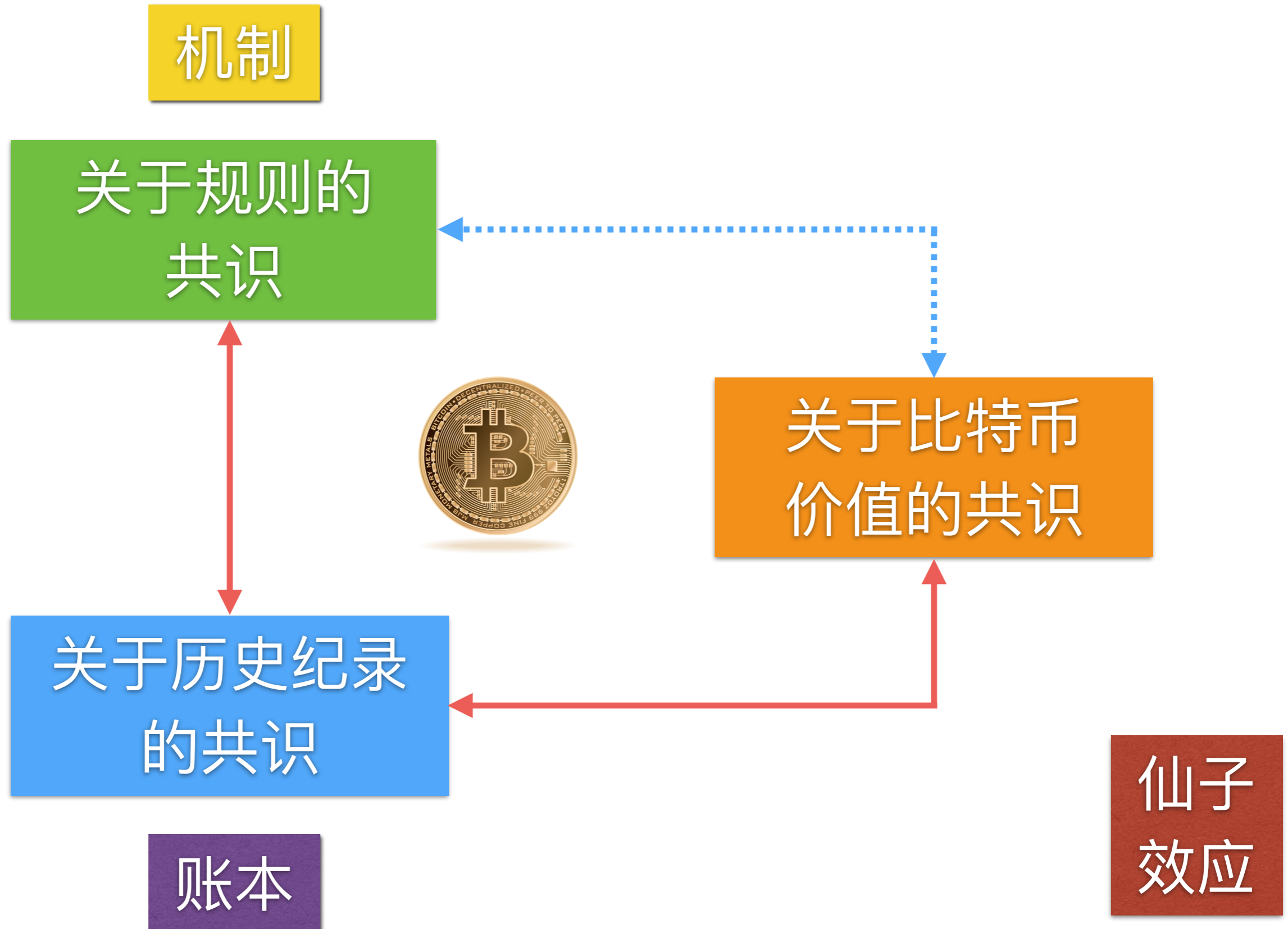
東京で MT.GOX のデモ
へ参加してください。
東京都渋谷区渋谷
2丁目 11-5

MTGOX
WHERE IS
OUR MONEY

- **10分钟**: 产生块的间隔
- **1M**: 一个块大小
- **2万签名**: 每个块
- **100M satoshi**: 每个币
- **21M**: 比特币数量
- **50、25、12.5....**: 挖矿奖励
- **250bytes**: 每个业务
- **7交易**: 每秒(*visa* 2千到1万, *Paypal* 50-100)

监管





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 and 代码

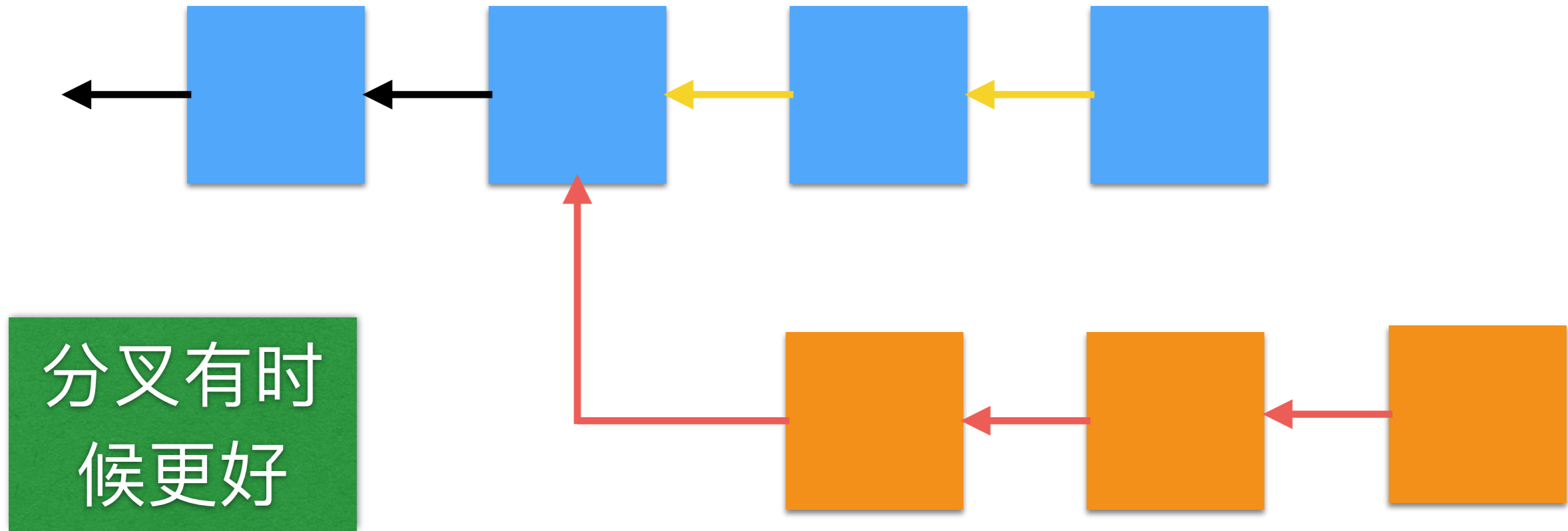
矿工：验证交易、编写历史纪录

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



分叉有时候更好

块大小

1M

2M

4M

8M

不限制



隔离见证

250/100

闪电网络

香港共识

SegWit

BIP141

BIP148

纽约共识

SegWit2x

BP91

UASF



The DAO 攻击



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
货币管理
政策

中国政府
2017年系列政策

日韩
新加坡

Welcomel | Silk Road


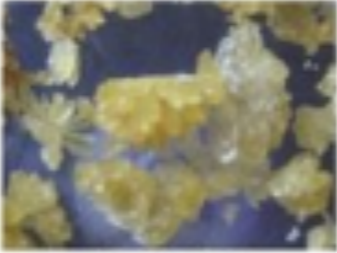







messages(0) | orders(0) | account(฿0.00) | settings | log out

Silk Road
anonymous marketplace

search | ฿(0)

Shop by category:

- Drugs(1249)
 - Cannabis(410)
 - Ecstasy(86)
 - Dissociatives(47)
 - Psychedelics(142)
 - Opioids(92)
 - Stimulants(107)
 - Other(150)
 - Benzos(96)
- Lab Supplies(23)
- Digital goods(93)
- Services(107)
- Money(71)
- Weaponry(9)
- Home & Garden(4)
- Food(1)
- Electronics(11)
- Books(76)
- Drug paraphernalia(46)
- XXX(48)
- Medical(3)
- Computer equipment(19)
- Art(1)
- Apparel(8)
- Sporting goods(3)
- Tickets(1)
- Forgeries(13)
- Fireworks(2)

 <p>1g Tangerine Kush Bubble Hash ฿60.96</p>	 <p>-NN- DMT YELLOW CLASSIC (500mg) ฿19.39</p>	 <p>Barcode Manipulation scam keeping... ฿2.31</p>
 <p>3.5g OG Kush ฿22.17</p>	 <p>MDMA and MDEA mixture 1 gram ฿23.44</p>	 <p>Guerrilla Warfare Book's ฿0.46</p>
 <p>co-codamol 30mg codeine / 500mg... ฿4.59</p>	 <p>CASH BLOWOUT!! Vendors, SYG is... ฿0.01</p>	 <p>"Super BOMB" Jolly Rancher 1/8... ฿24.20</p>

News:

- Site glitches
- Missing deposits
- Site restored
- Forum bugs addressed
- Pricing and hedging improvements
- Escrow hedging update
- New feature to help protect sellers
- Seller ranking and feedback overhaul



把现实世界和虚拟世界完全分离是很困难的

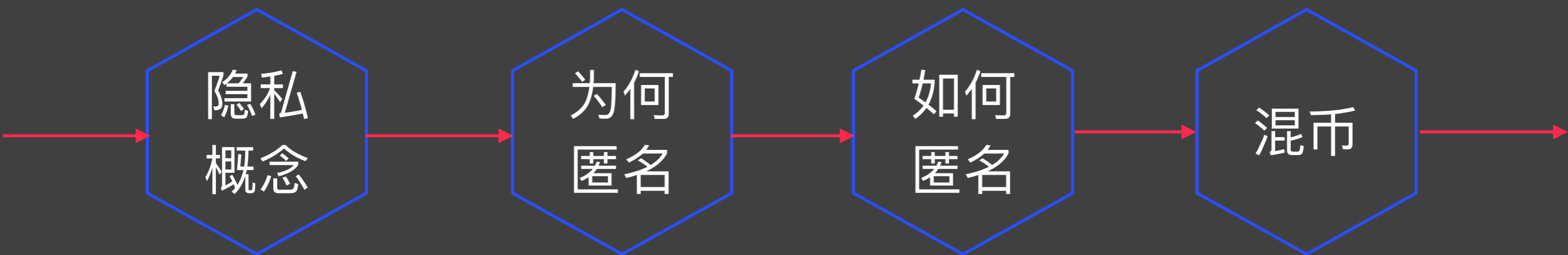
匿名

隐私
概念

为何
匿名

如何
匿名

混币



比特币是安全的匿名的
加密货币

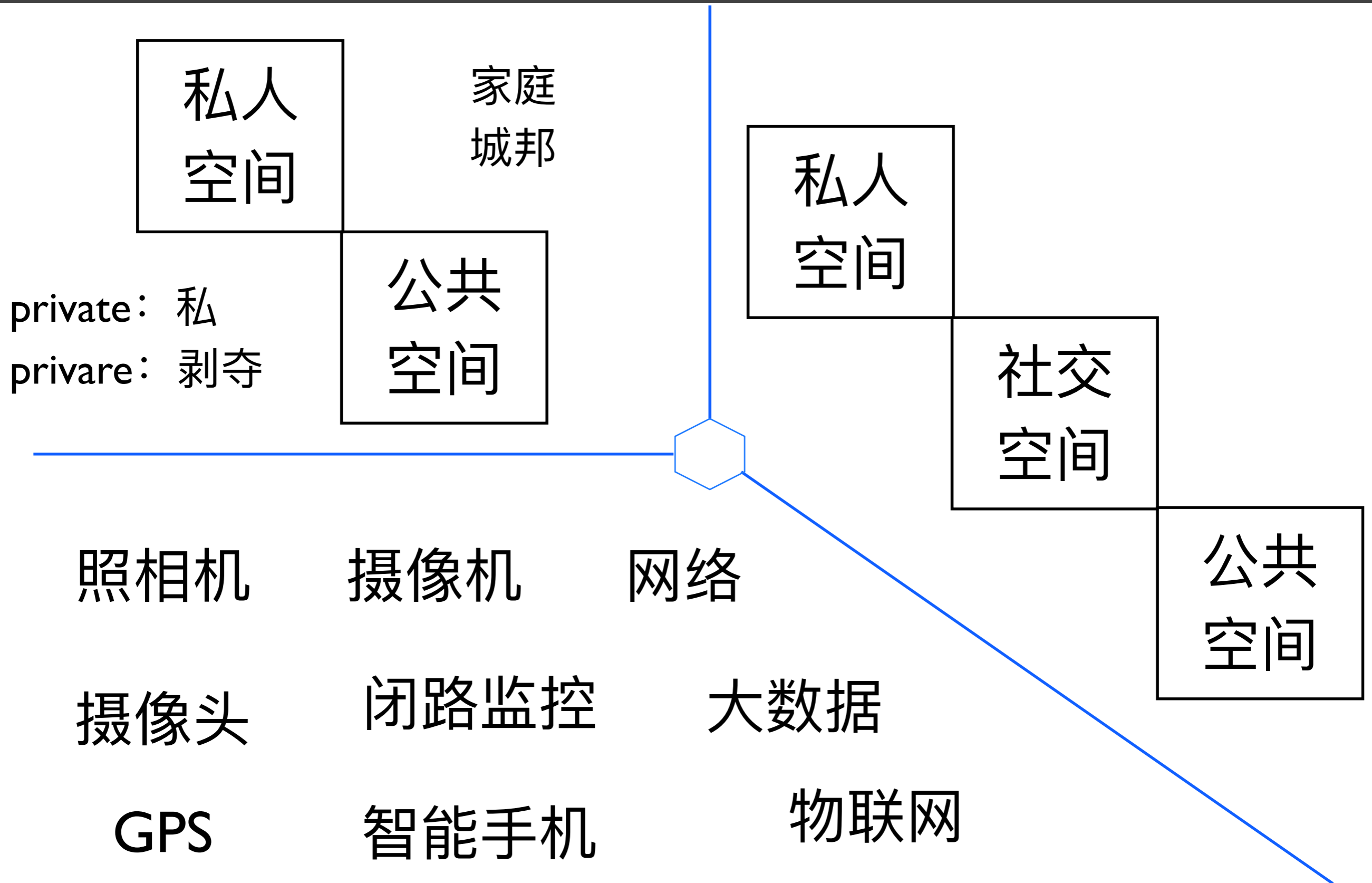
比特币不能帮你逃
脱NSA的监控

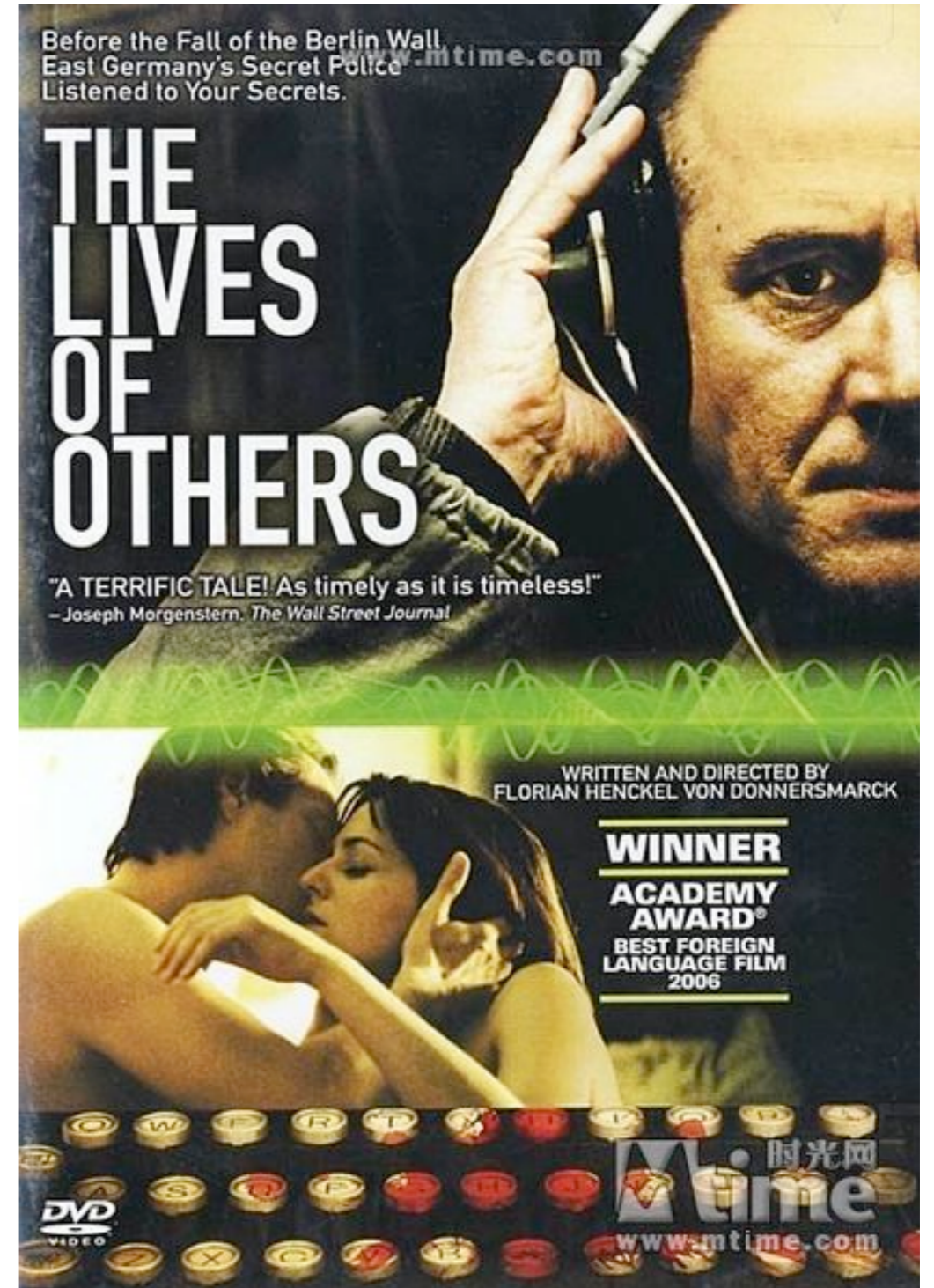
- 任何人的私生活、家庭、住宅和通信不得任意干涉，他的荣誉和名誉不得加以攻击，人人有权享受法律保护，以免受这种干涉和攻击。



**The Right to be Let
Alone**

隐私：正面和方面







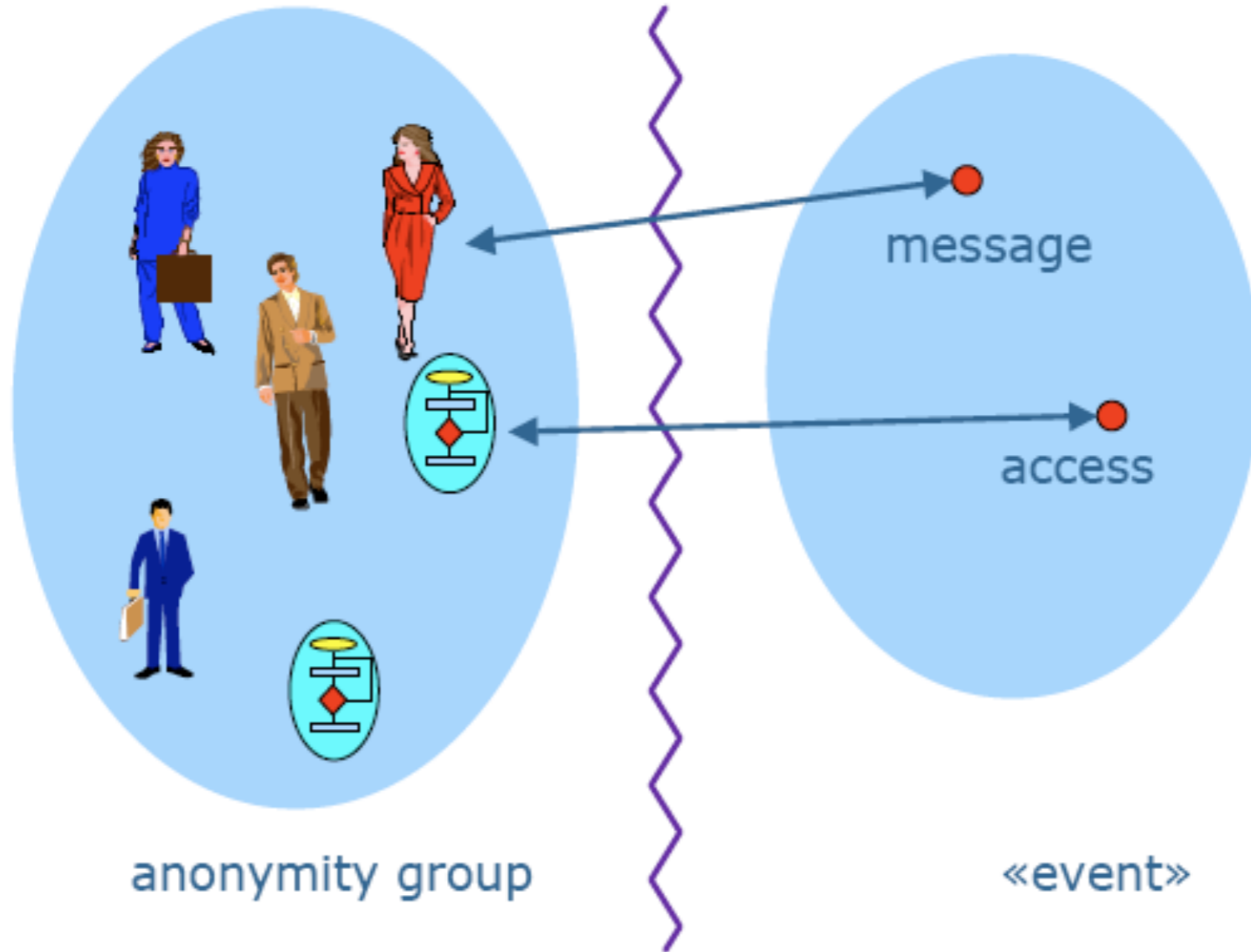
<http://maher-arar.net/>



Cambridge Analytica



Google:
Don't be evil.



无关联性

- 匿名：没有名字
 - * 交易的时候不使用真实的姓名
 - * 交易的时候完全不使用任何名字
- 比特币使用公钥Hash作为地址
- CS：匿名 = 化名 + 无关联性
- 比特币具有化名性
- 把比特币地址和真实身份关联起来并不困难

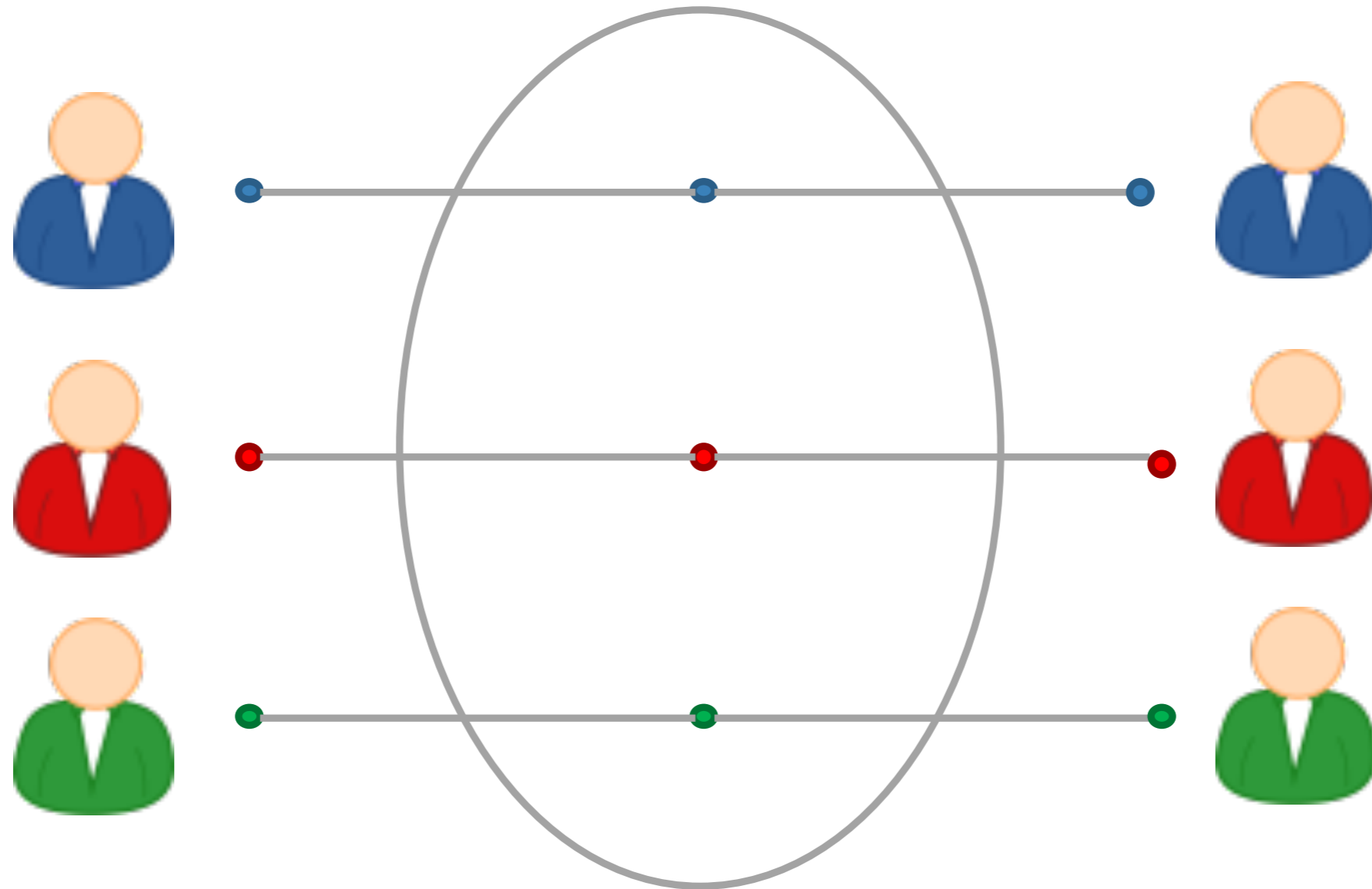
- 比特币的交易信息是公开的
 - 旁路攻击、污点分析、匿名集合(定量)
 - 匿名的好坏、匿名的道德评判(洗钱等)
-
- 同一个用户的不同地址应该不易关联
 - 同一个用户的不同交易应该不易关联
 - 同一个交易的交易双方应该不易关联

数据
脱敏

匿名
集合

Name	Age	Gender	State of domicile	Religion	Disease
Ramsha	29	Female	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	Kerala	Hindu	Viral infection
Salima	28	Female	Tamil Nadu	Muslim	TB
sunny	27	Male	Karnataka	Parsi	No illness
Joan	24	Female	Kerala	Christian	Heart-related

Name	Age	Gender	State of domicile	Religion	Disease			
Bahuksana	23	Male						
Rambha	19	Male	*	20 < Age ≤ 30	Female	Tamil Nadu	*	Cancer
Kishor	29	Male	*	20 < Age ≤ 30	Female	Kerala	*	Viral infection
Johnson	17	Male	*	20 < Age ≤ 30	Female	Tamil Nadu	*	TB
John	19	Male	*	20 < Age ≤ 30	Male	Karnataka	*	No illness
			*	20 < Age ≤ 30	Female	Kerala	*	Heart-related
			*	20 < Age ≤ 30	Male	Karnataka	*	TB
			*	Age ≤ 20	Male	Kerala	*	Cancer
			*	20 < Age ≤ 30	Male	Karnataka	*	Heart-related
			*	Age ≤ 20	Male	Kerala	*	Heart-related
			*	Age ≤ 20	Male	Kerala	*	Viral infection

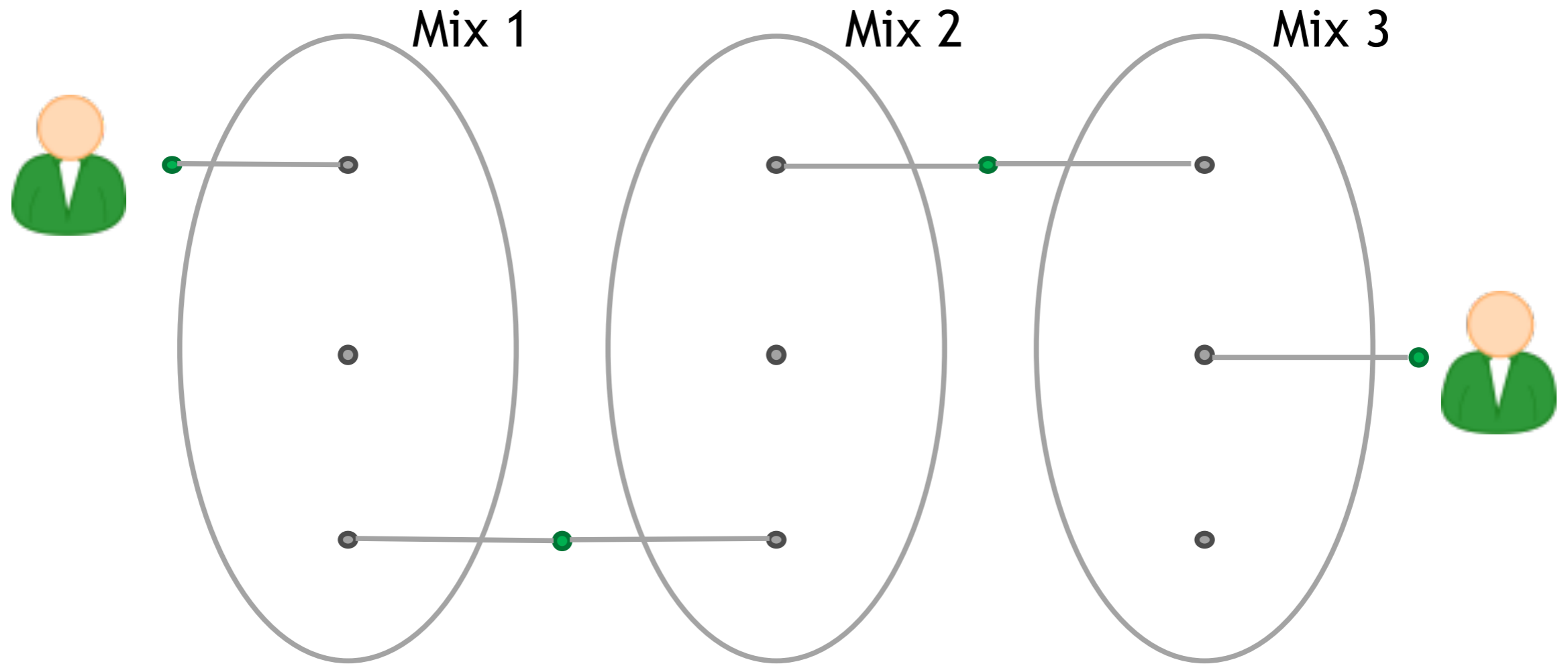


在线钱包

引入中介节点

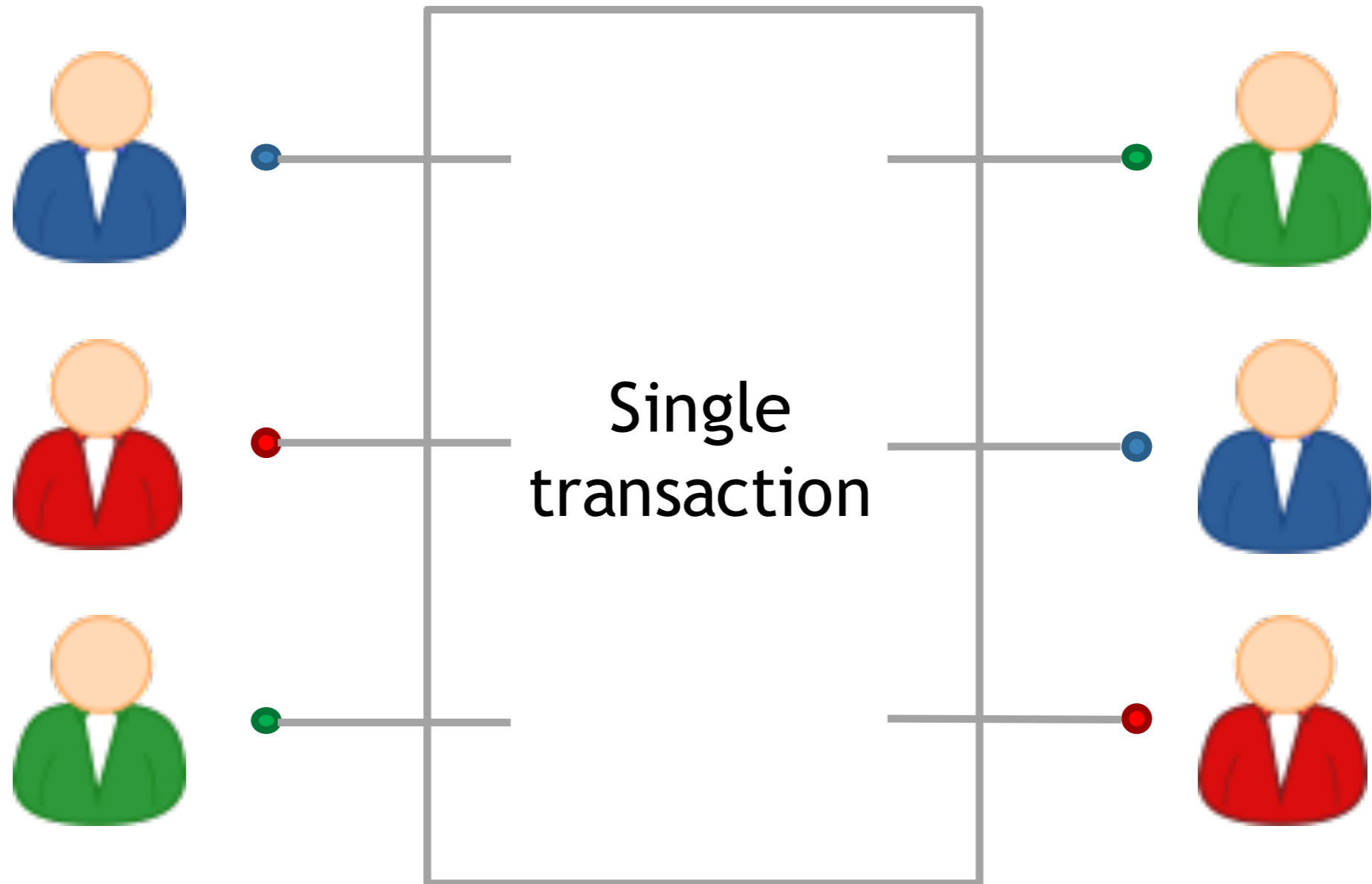
专项服务

多层混币



多重

分布式混币



分布式

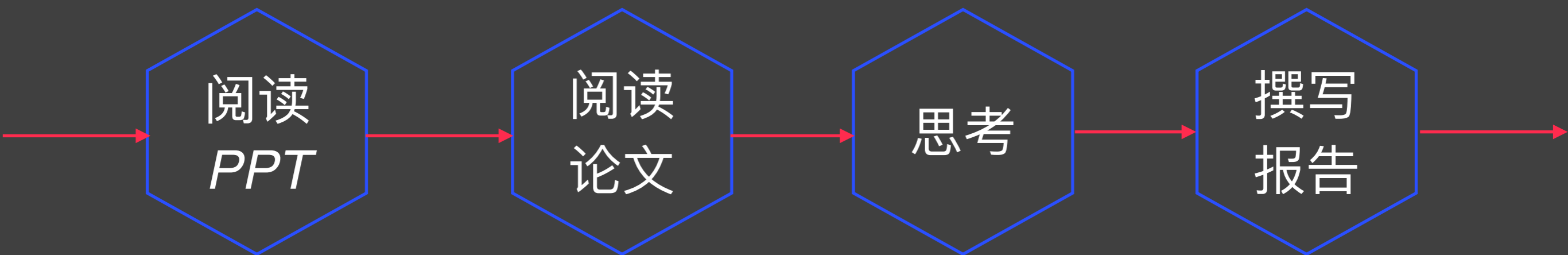
课后作业

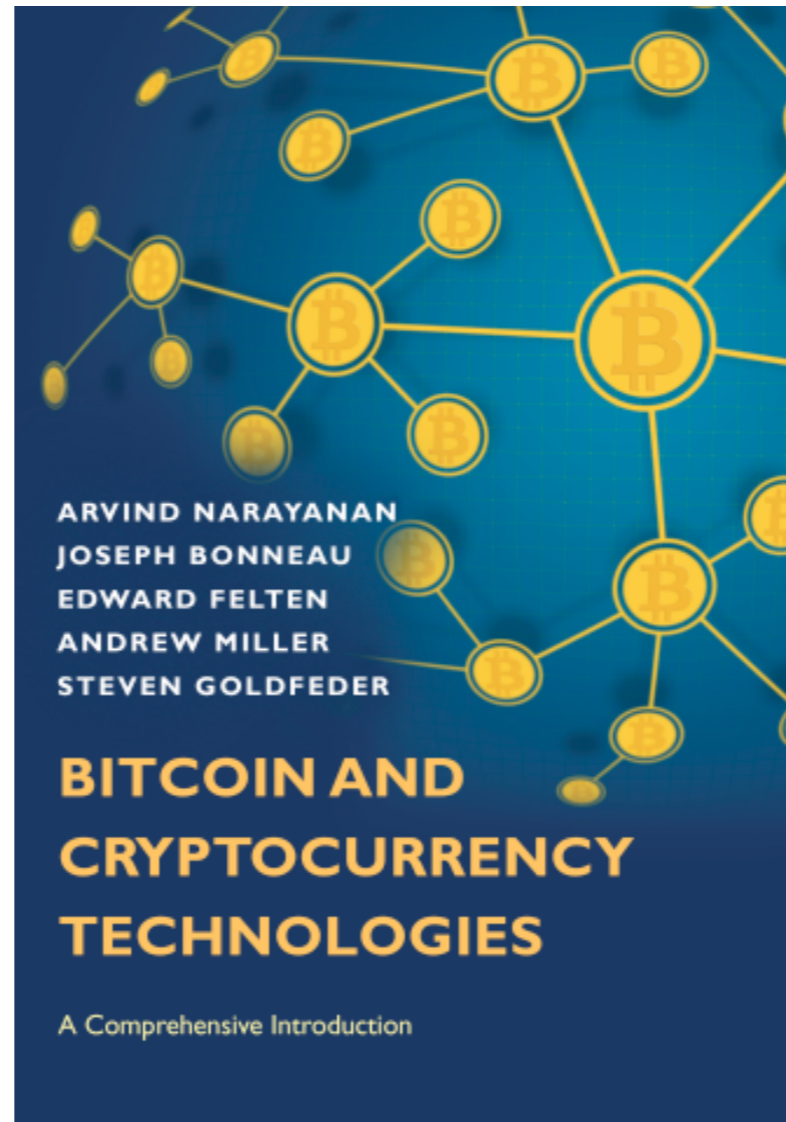
阅读
PPT

阅读
论文

思考

撰写
报告





阅读第1-7章

要求阅读如下文章，写阅读报告

1432

IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 22, NO. 2, SECOND QUARTER 2020

A Survey of Distributed Consensus Protocols for Blockchain Networks

Yang Xiao^{ID}, *Student Member, IEEE*, Ning Zhang^{ID}, *Member, IEEE*, Wenjing Lou^{ID}, *Fellow, IEEE*,
and Y. Thomas Hou^{ID}, *Fellow, IEEE*

COMST'2020

<https://ieeexplore.ieee.org/abstract/document/8972381>

检索一篇区块链共识算法的好文章
好的会议和期刊：参见CCF列表

- 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

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

<https://huipingsun.github.io>