

# 区块链技术 II



# 上次课程内容

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

# 本次课程内容

## 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

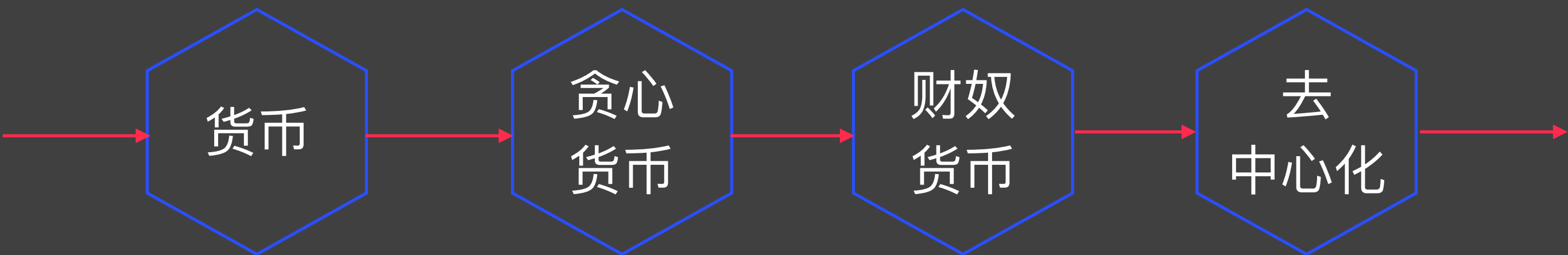
## 3 匿名

- 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

# 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**

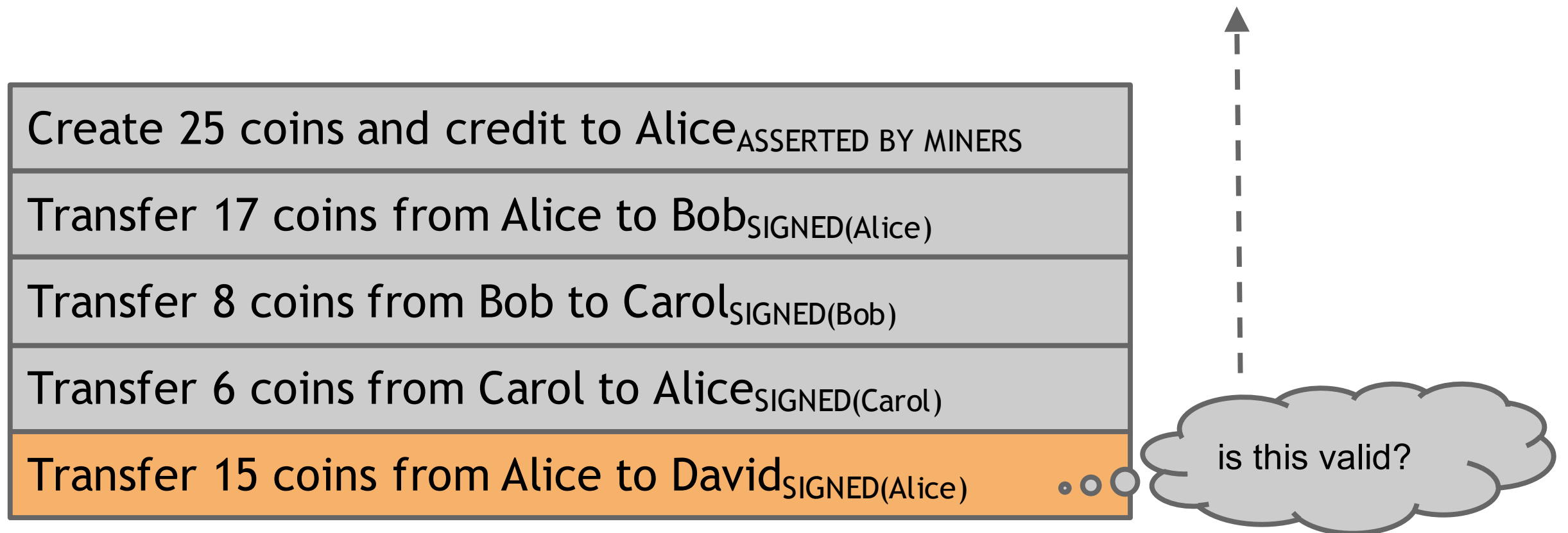
2015年版第5套人民币100元纸币在保持2005年版第五套人民币100元纸币规格、正背面主图案、主色调、“中国人民银行”行名、国徽、盲文和汉语拼音行名、民族文字等不变的前提下，对部分图案做了调整，对整体防伪性能进行了提升。

- 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，该安全线中正反交替排列的镂空文字“¥100”。
- 2 雕刻凹印**  
票面正毛泽东头像、国徽、“中国人民银行”行名、左上角面额数字、盲文及背面人民大会堂等均采用雕刻凹印印刷，用手触摸时有明显的凹凸感。
- 3 数字对印图案**  
票面正面左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 水印**  
位于票面正面左侧下方。透光观察，可以看到透光很强的水印图案数字“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，其前两位数字为暗红色，后六位数字为黑色；右侧竖号码为黑色。



广发银行  
CGB

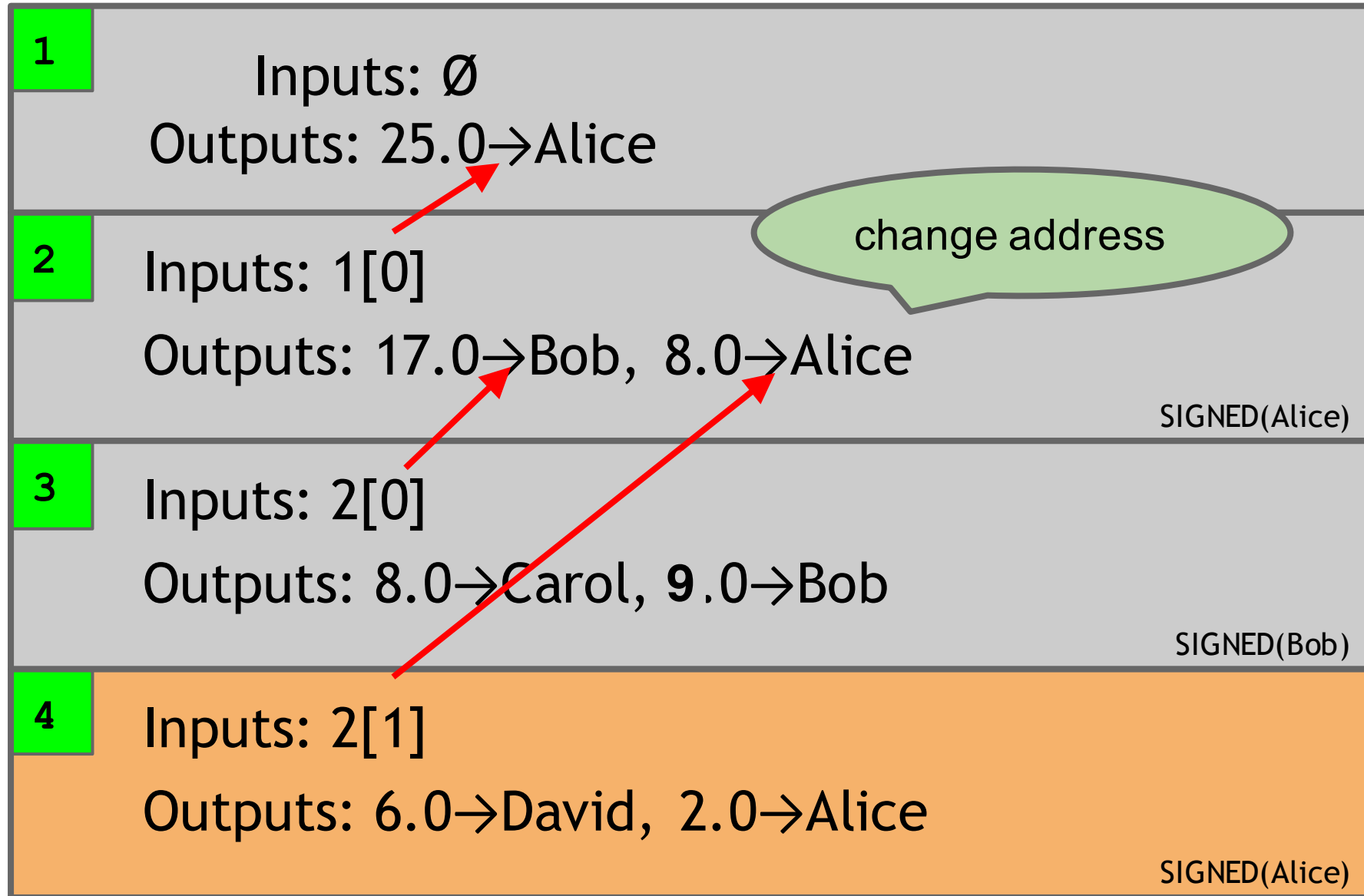
时间



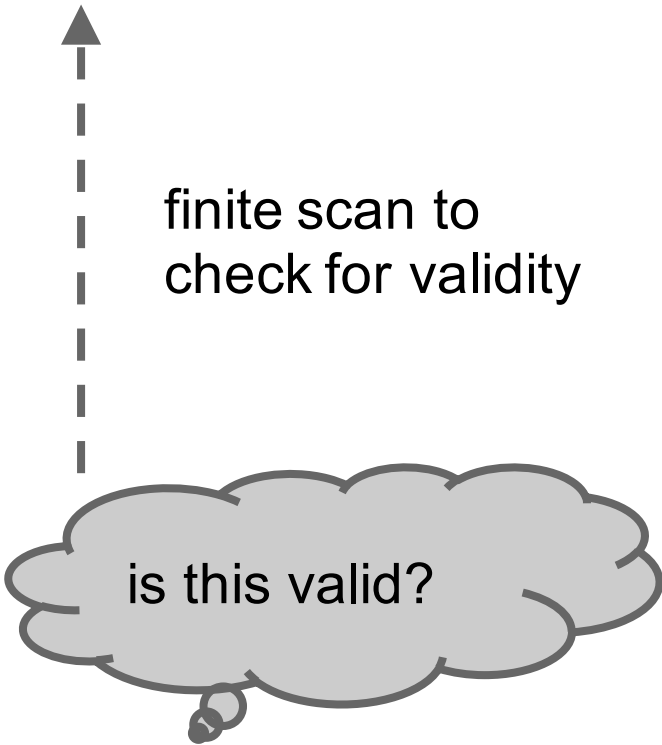
一个块包含一个交易

交易验证需要扫描以前所有的块

时间



we implement this with hash pointers



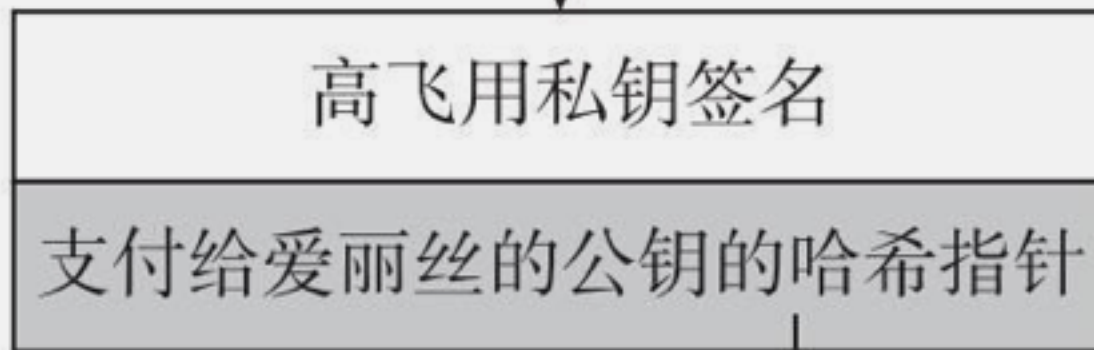
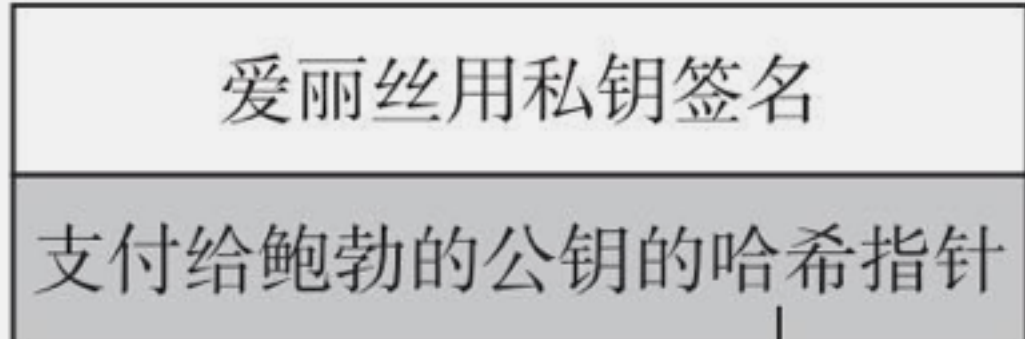
一个块包含一个交易

交易验证需要扫描以前所有的相关块



# 高飞币

爱丽丝支付给  
查克



双重花费

# 贪心币



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

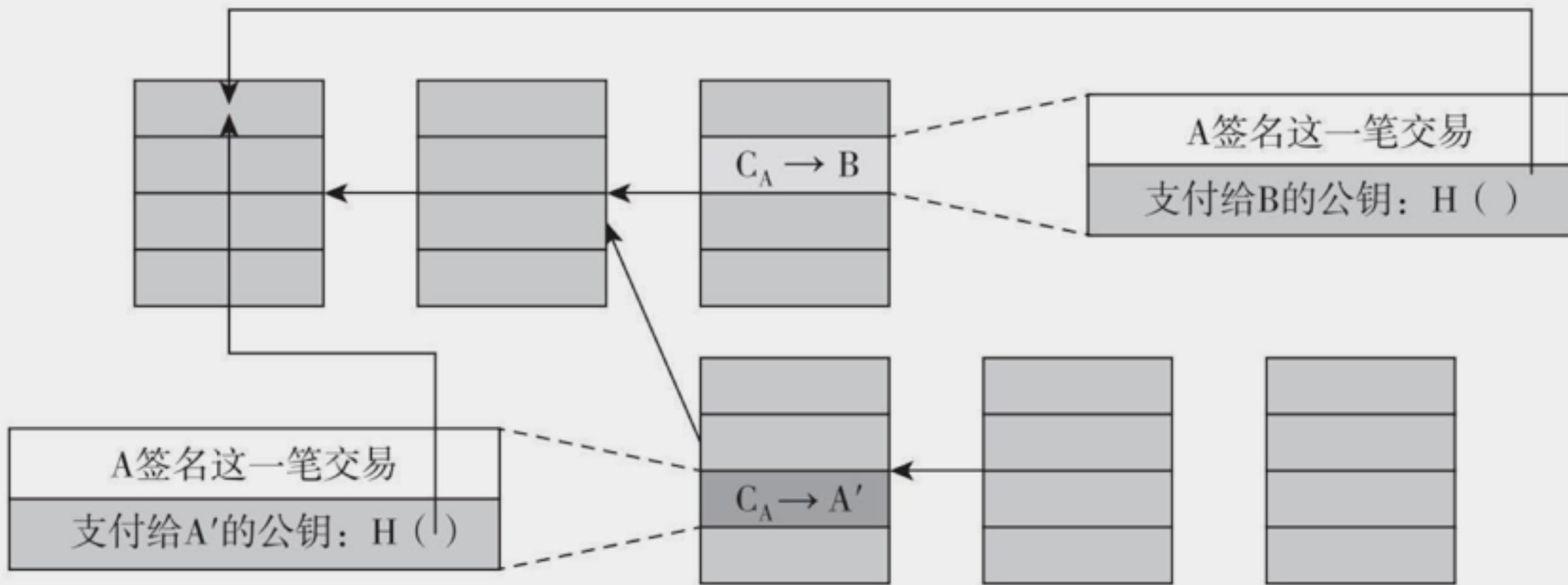
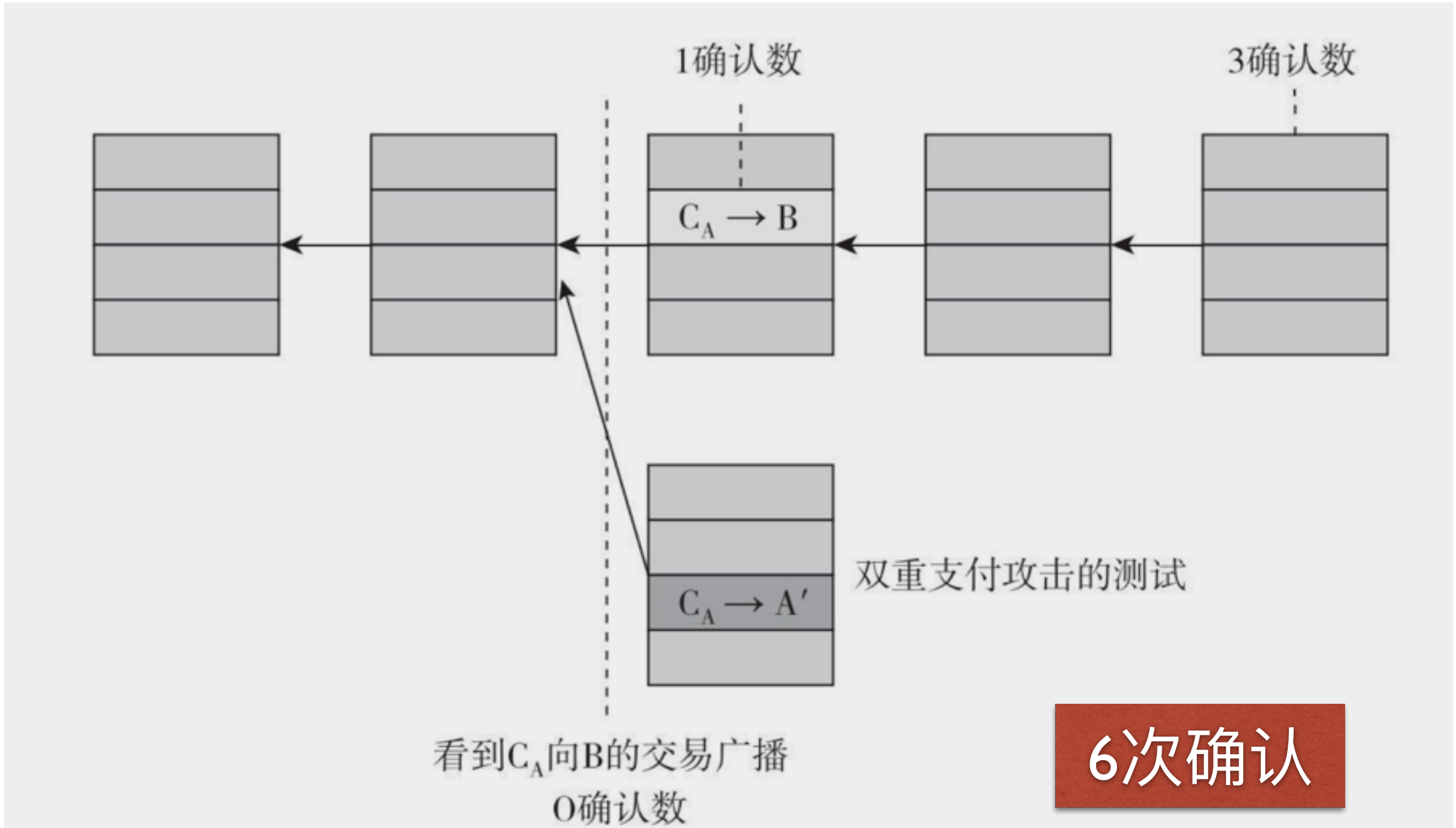


图2.2 双重支付攻击

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。

# 双重攻击防止：等待多次确认



看到 $C_A$ 向B的交易广播  
0确认数

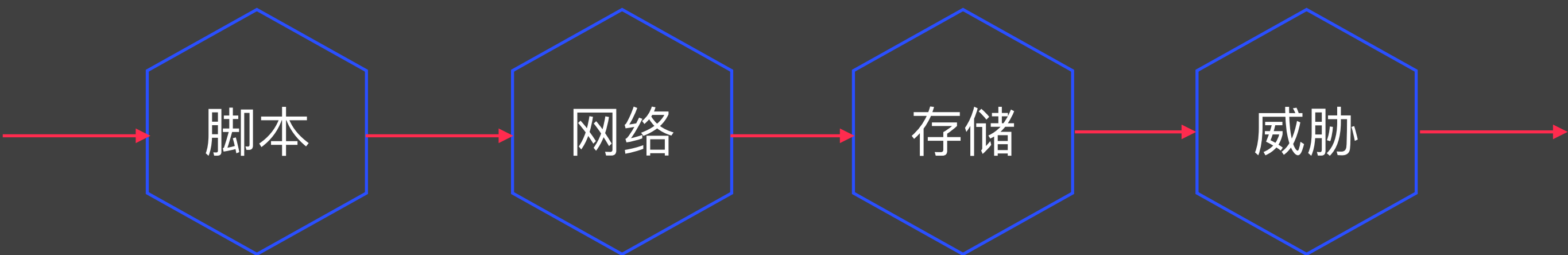
**6次确认**

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



# 比特币脚本

```
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
```

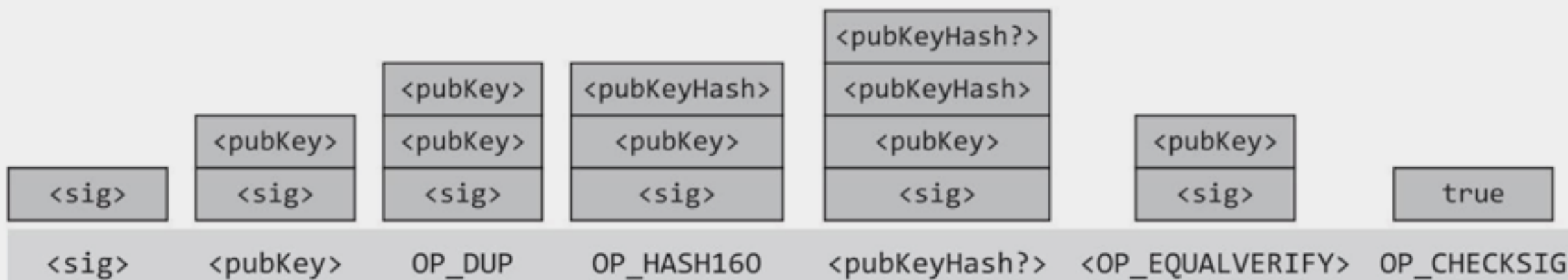


图3.6 比特币脚本的执行堆栈状态图

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。

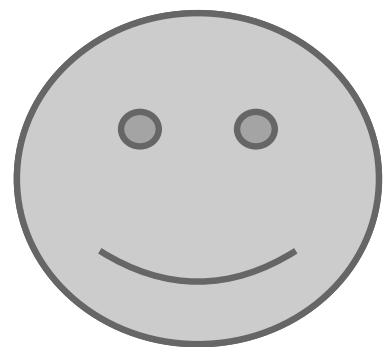
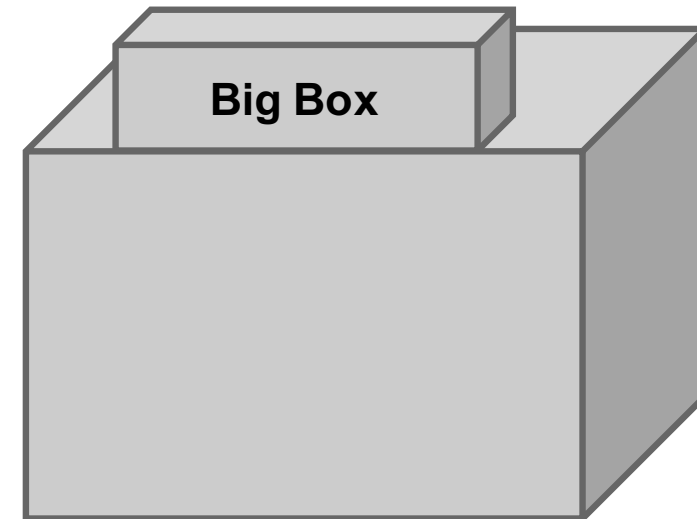
# P2SH



I'm ready to pay for my purchases!



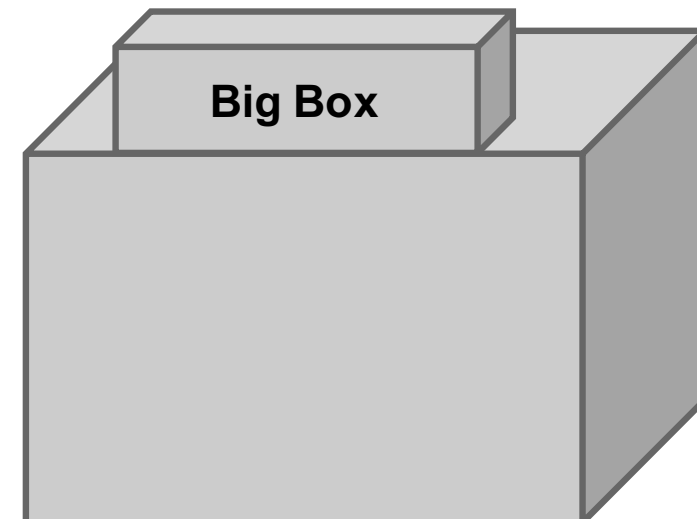
Cool! Well we're using MULTISIG now, so include a script requiring 2 of our 3 account managers to approve. Don't get any of those details wrong. Thanks for shopping at Big Box!



I'm ready to pay for my purchases!



Great! Here's our address: 0x3454



# 比特币交易程序

```
{
  "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

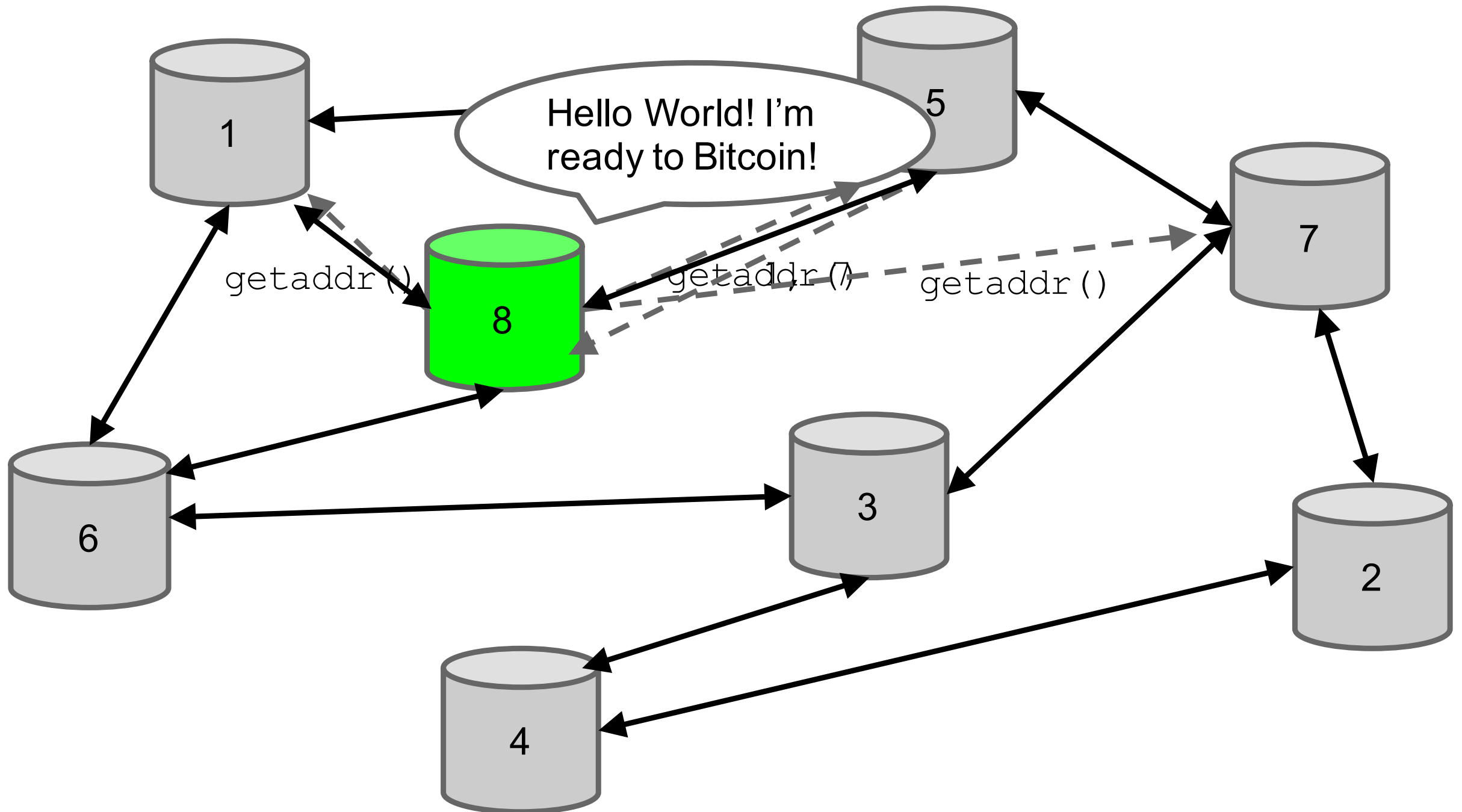
输入

输出

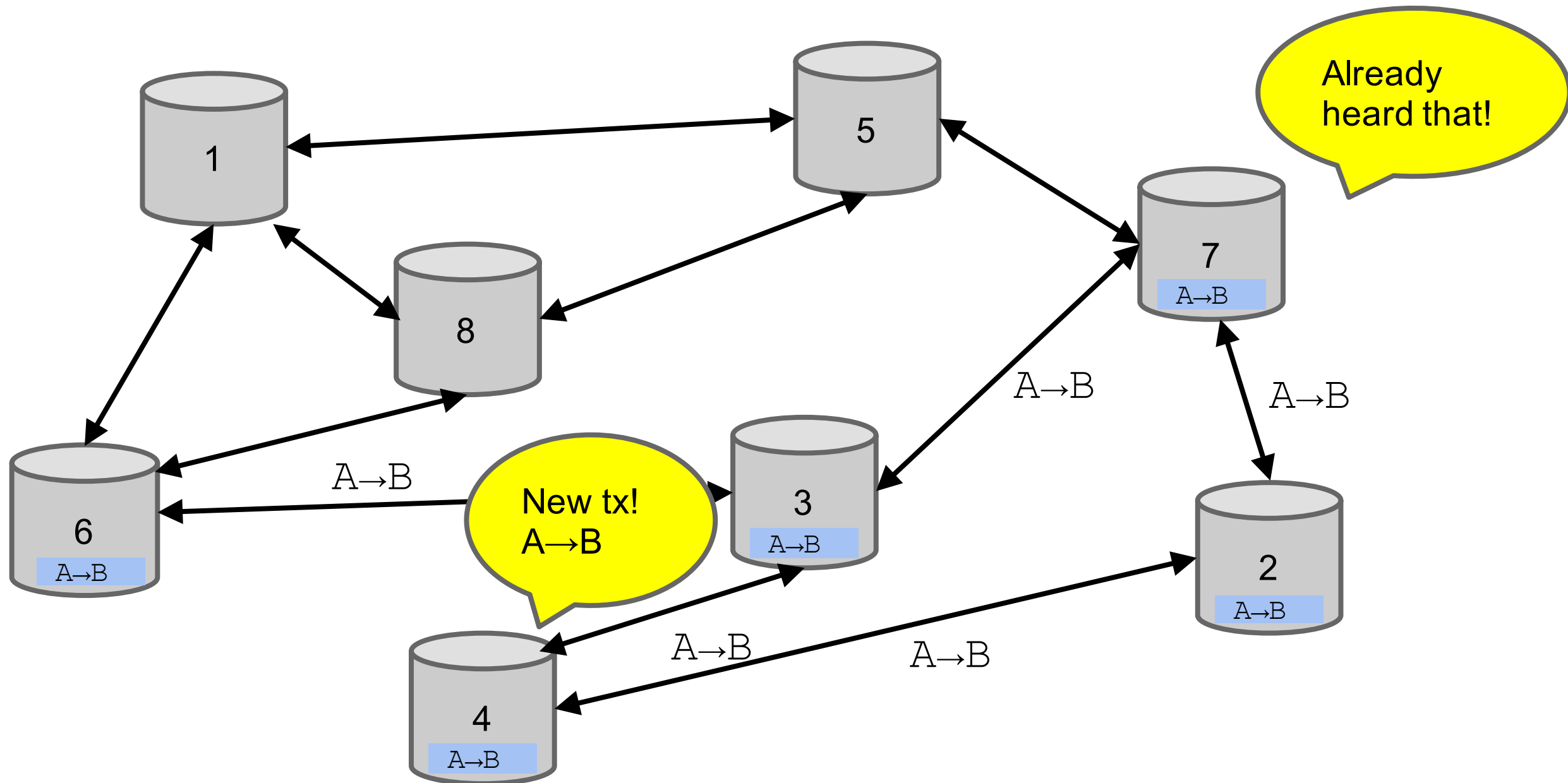
图3.3 一个真实的比特币交易程序段

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

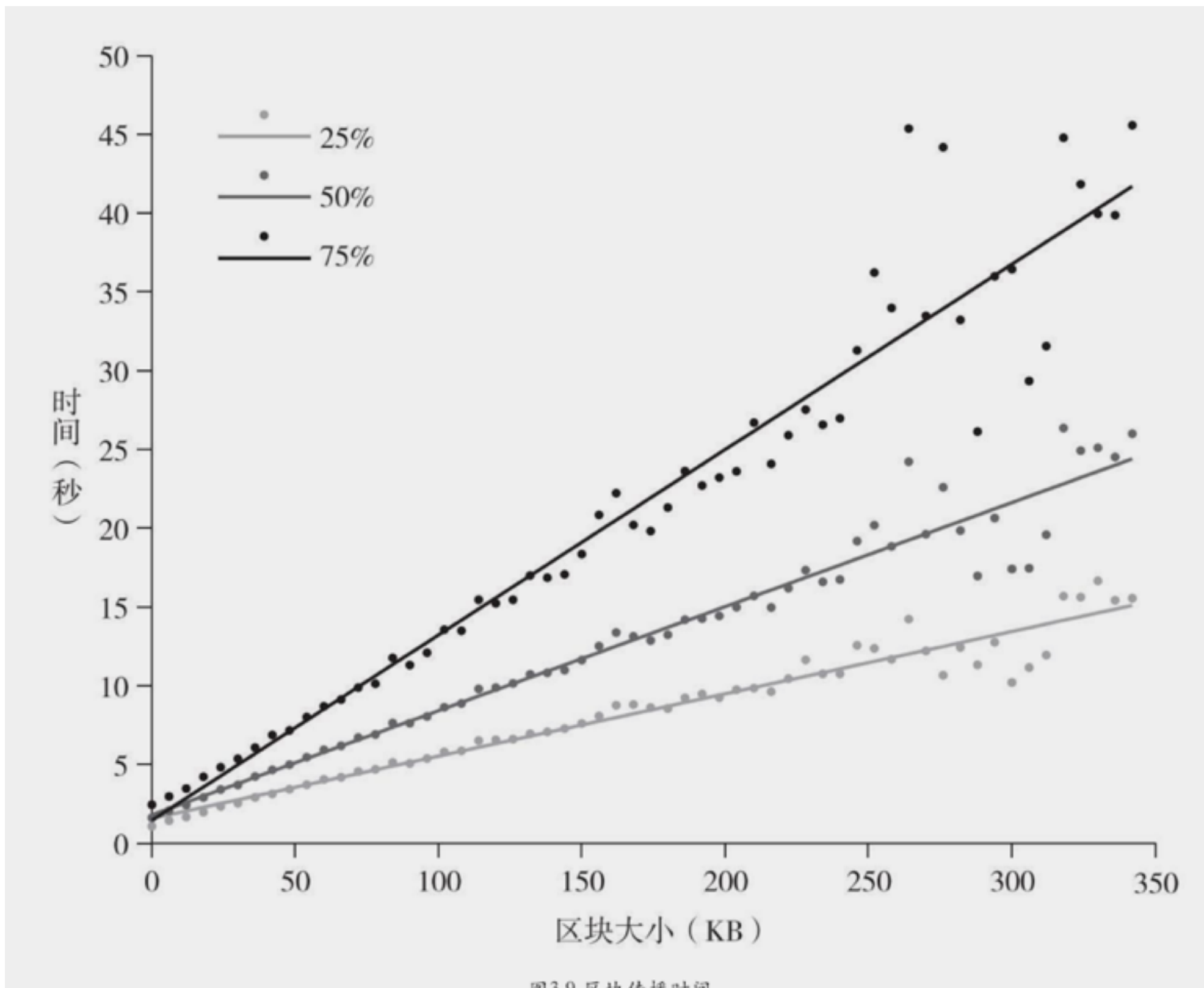
图3.8 币基交易



# 比特币网络交易消息传播



# 块传播





# 存储花费

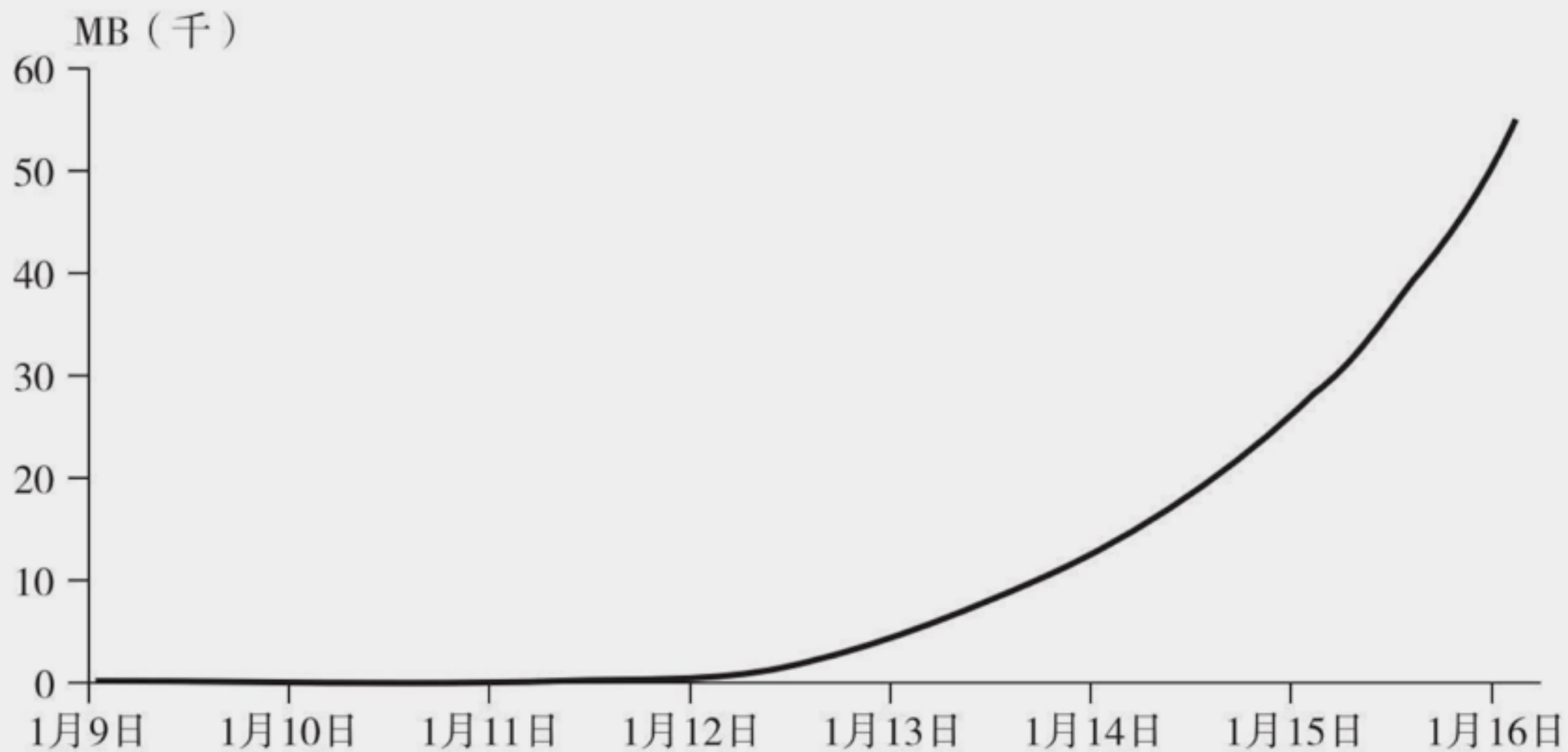
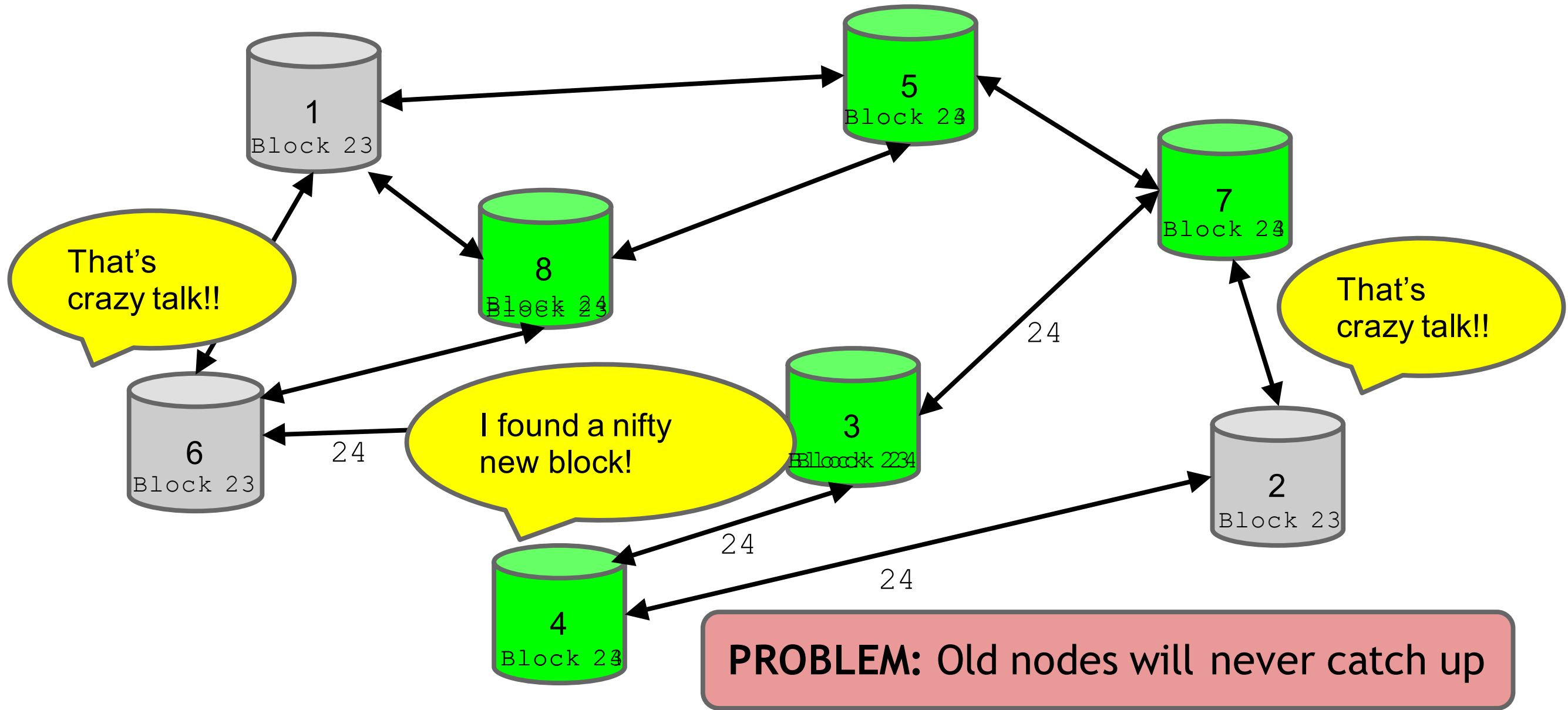


图3.10 区块链的大小

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。

# 分叉



硬 vs. 软

## Hot storage



online

hot secret key(s)

cold address(es)

## Cold storage



offline

payments





Charles Ponzi







- **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)**

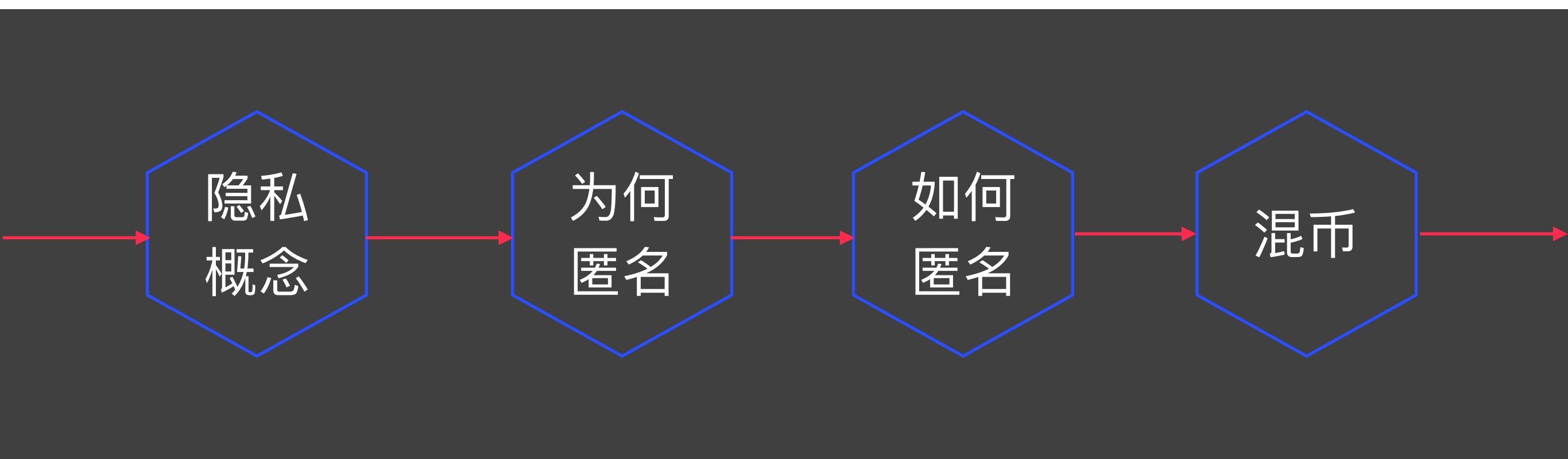
# 匿名

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

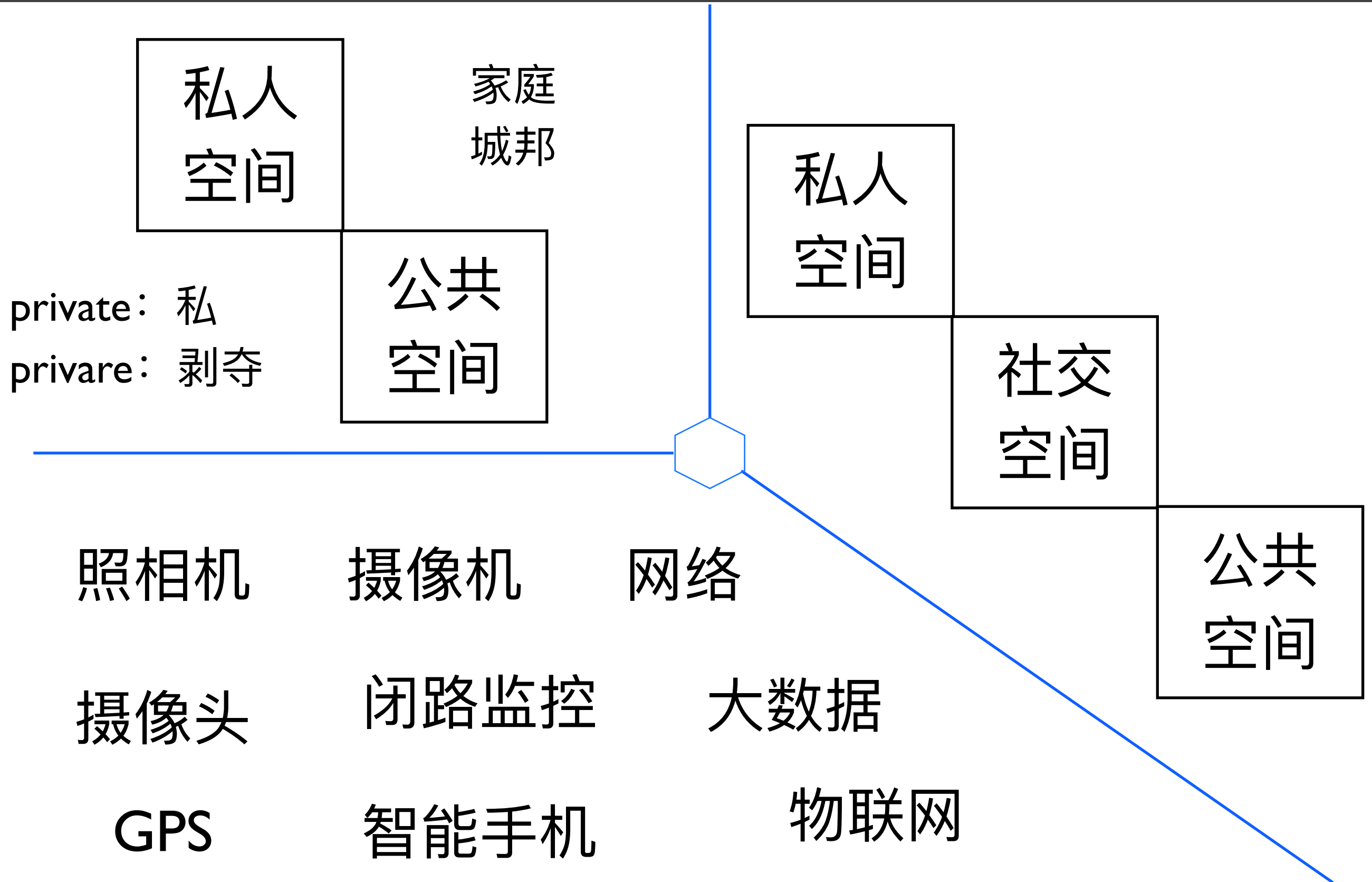


- 任何人的私生活、家庭、住宅和通信不得任意干涉，他的荣誉和名誉不得加以攻击，人人有权享受法律保护，以免受这种干涉和攻击。

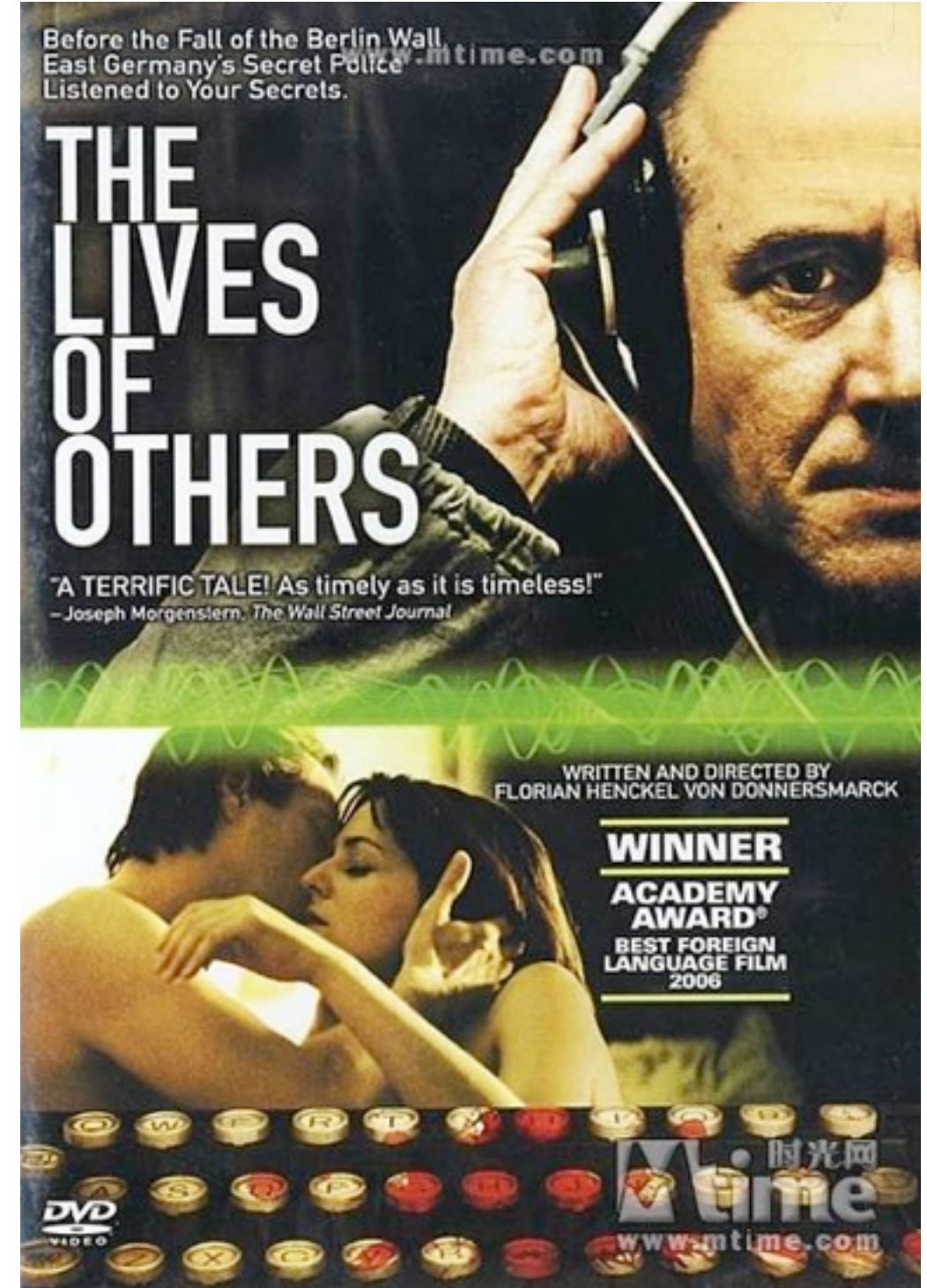


**The Right to be Let Alone**

# 隐私：正面和方面









隐私： 相关事件



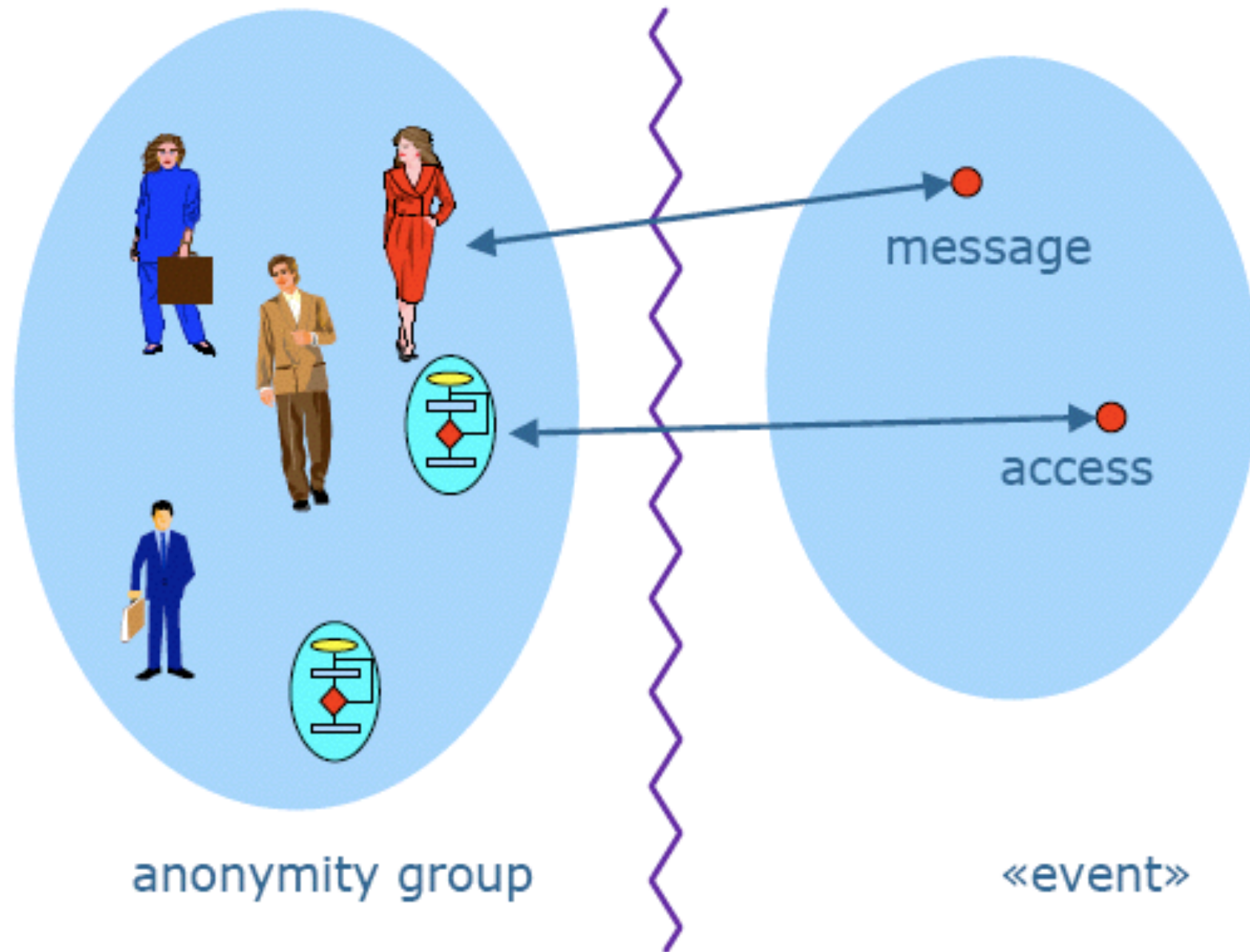
<http://maherarar.net/>



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

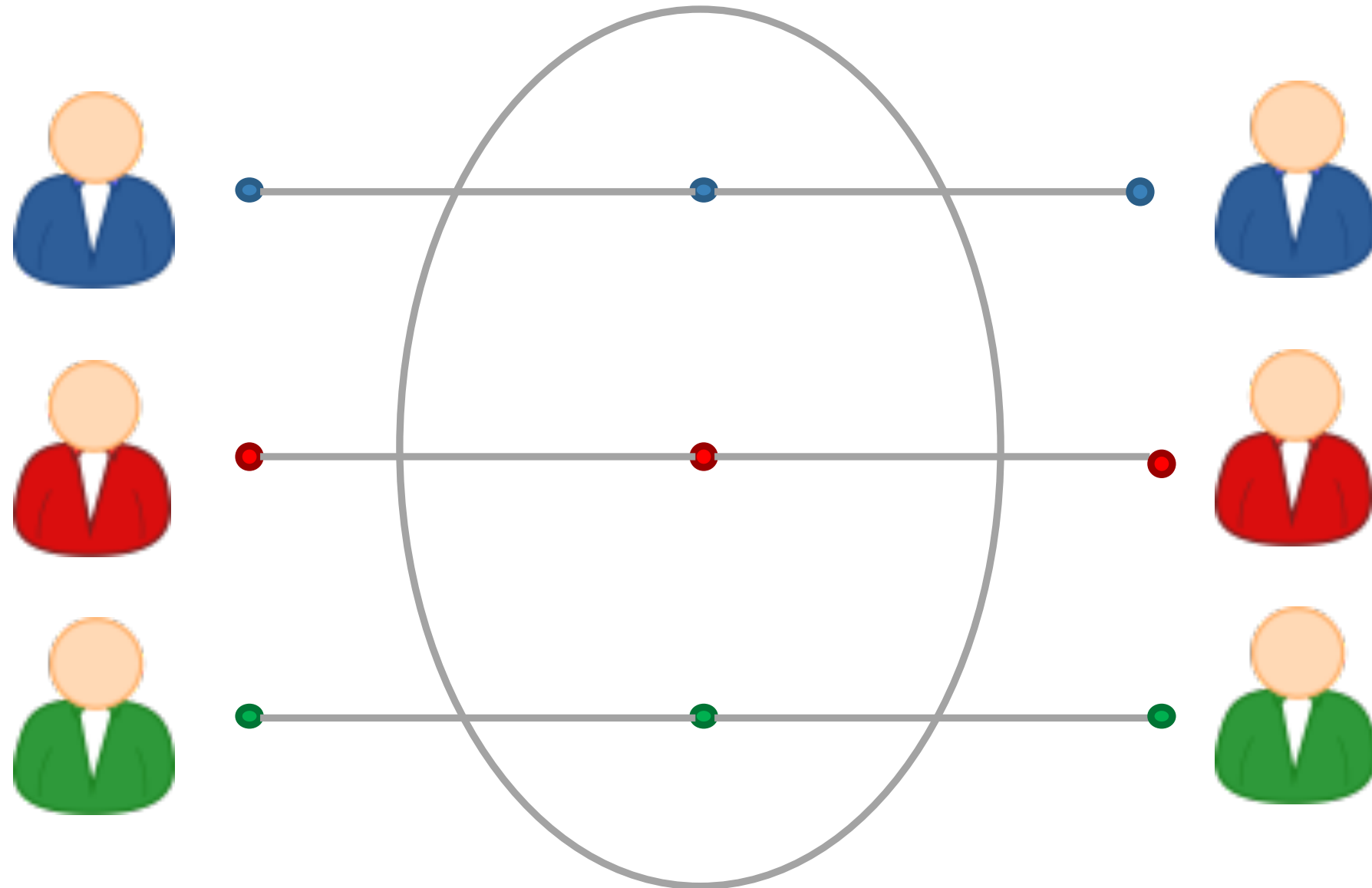
匿名  
集合

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



# 混币模式

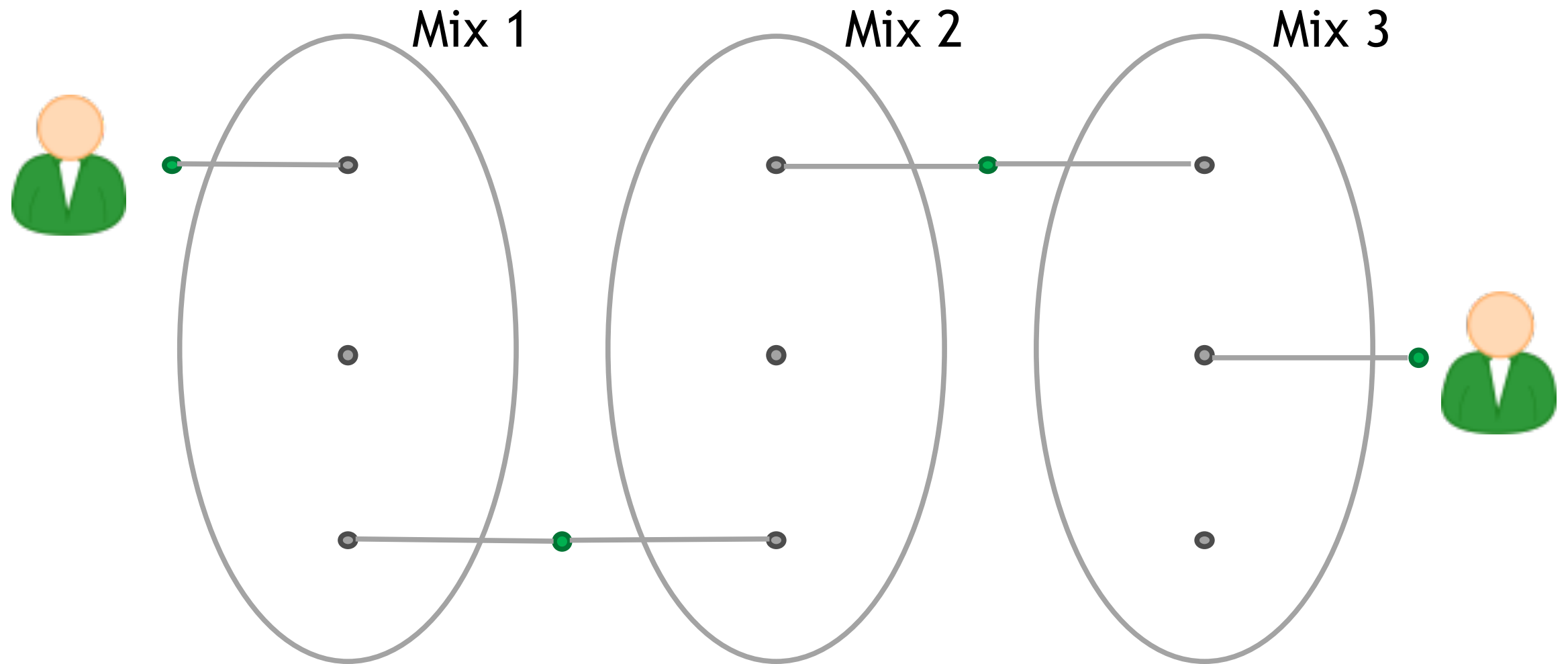


在线钱包

引入中介节点

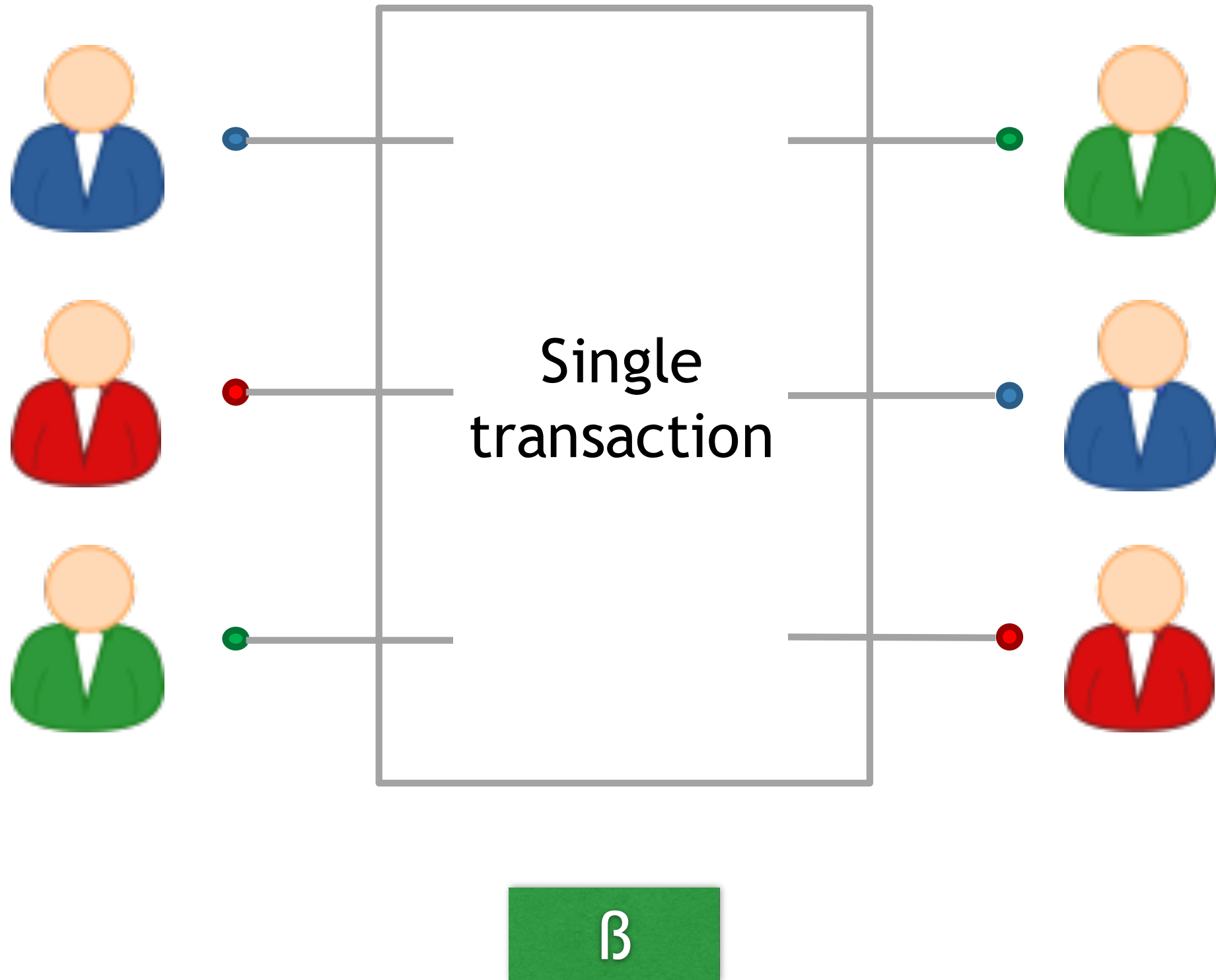
专项服务

# 多层混币

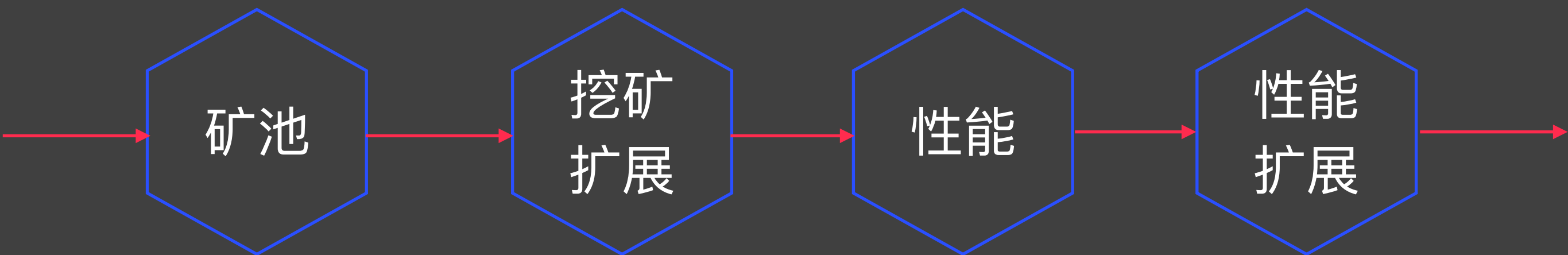


多重

# 分布式混币



# 扩展



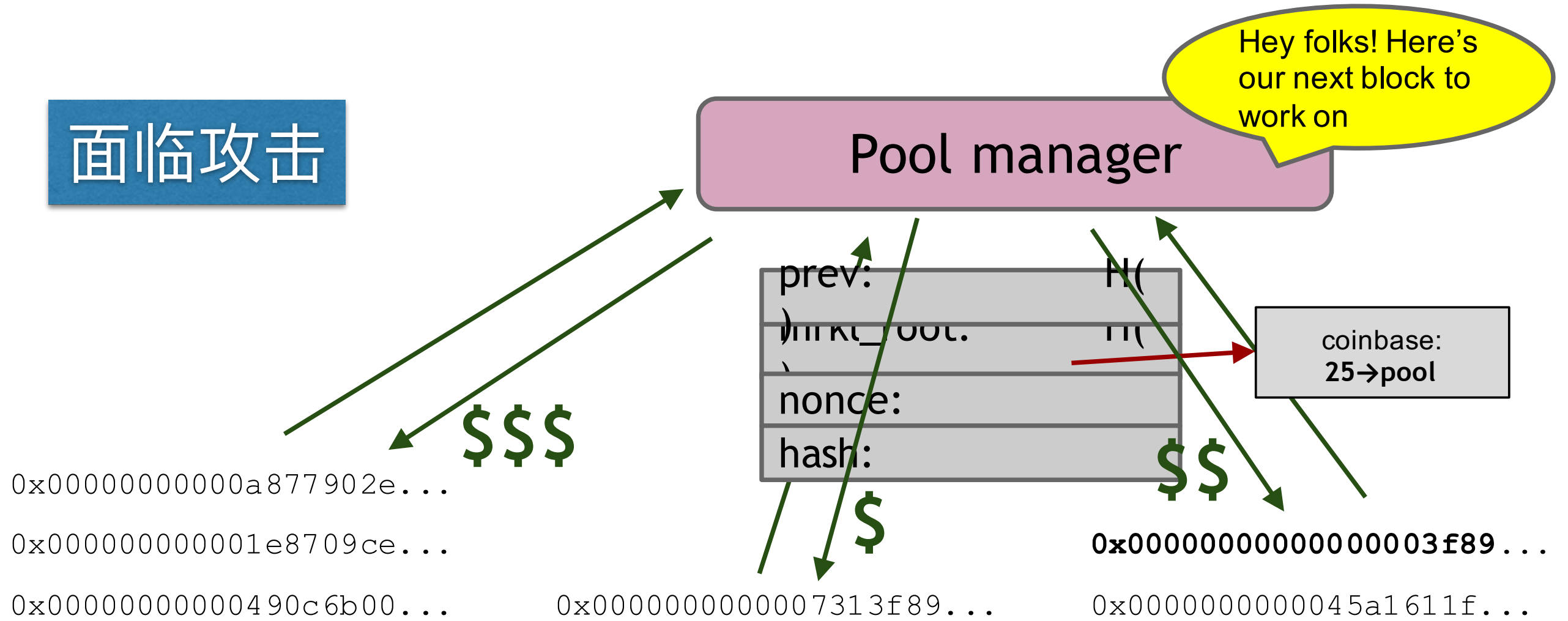


输出接近结果的挖矿结果来证明自己的工作量

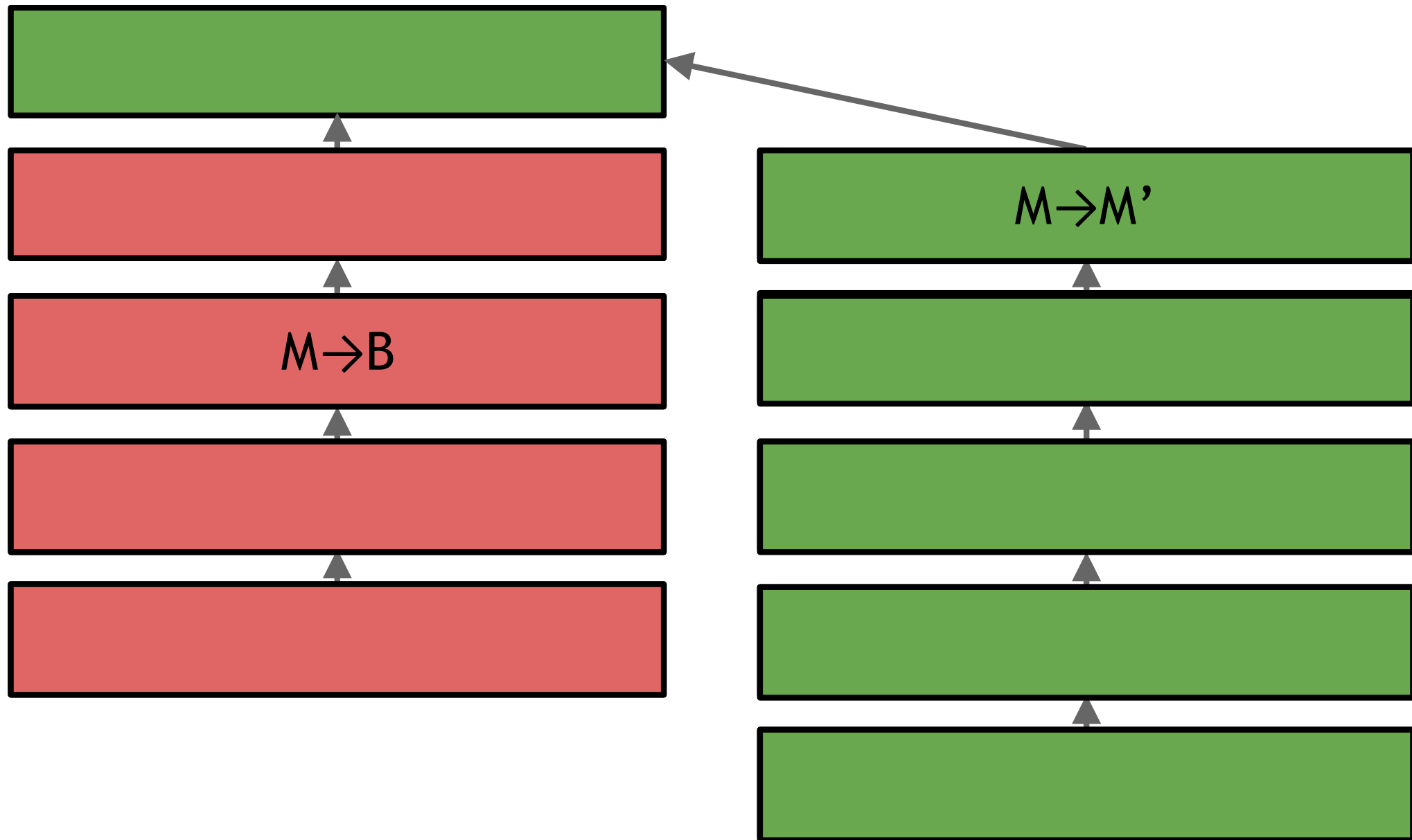
```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB  
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD  
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255  
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B  
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF  
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1  
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB  
000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A  
652F374601D149AC47E01E7776138456181FA4F9D0EEDD8C4FDE3BEF6B1B7ECE  
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3  
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5  
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```



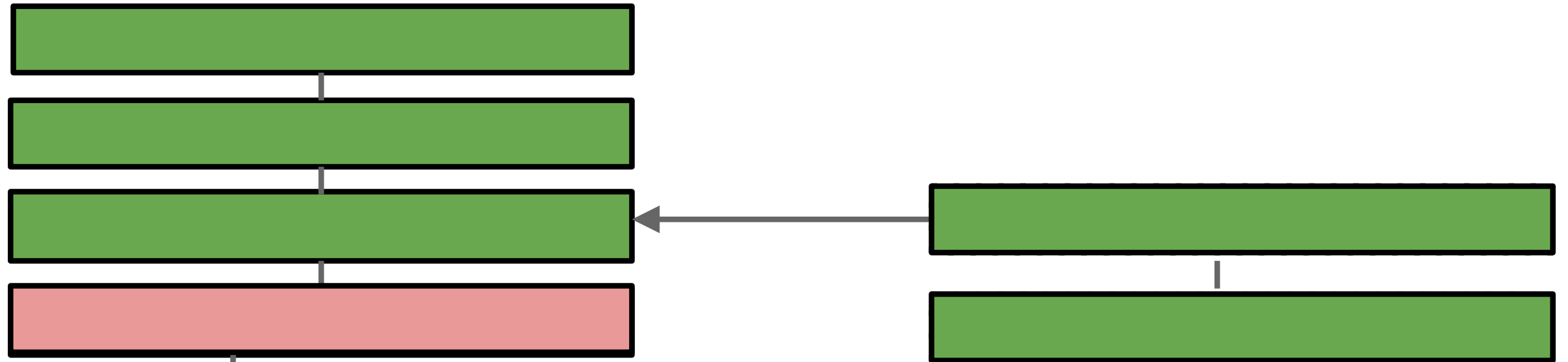
面临攻击



# 分叉攻击



# 临时保留区块攻击



All other miners are  
wasting effort here!

# 挖矿算法基本要求

挖矿算法是比特币系统的核心

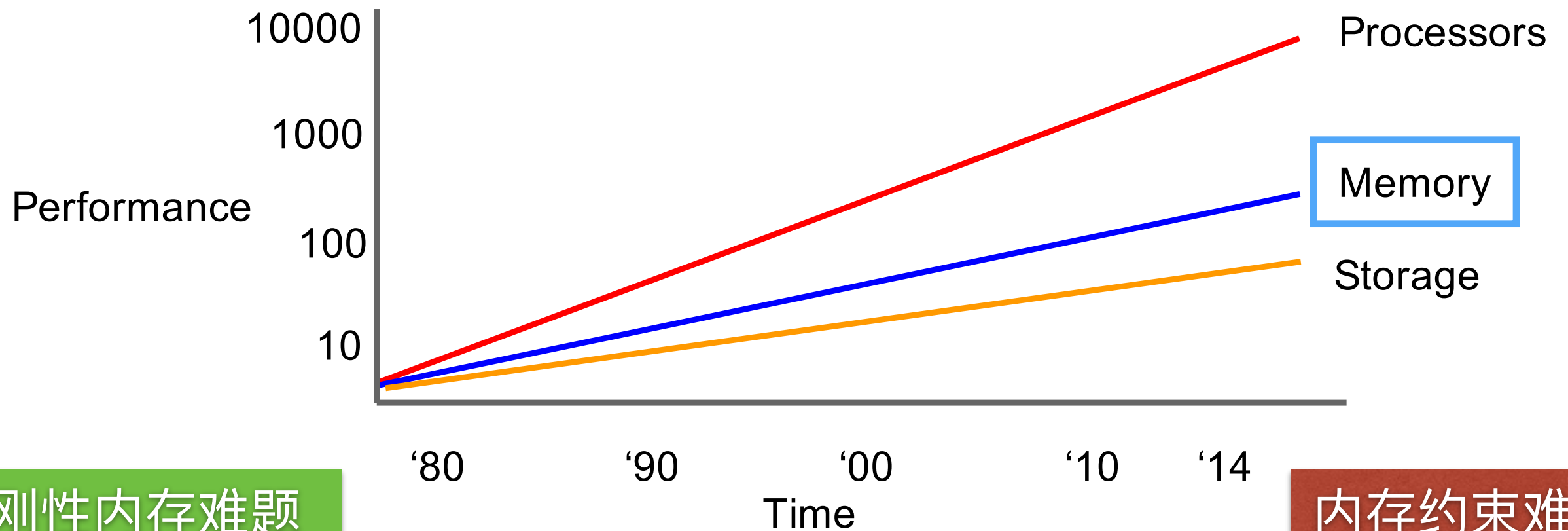
需要一个难题  
计算复杂

挖矿难题的结果要求验证简单

挖矿难题的难度可调节的特性

成功概率和所贡献的算力成比例





刚性内存难题

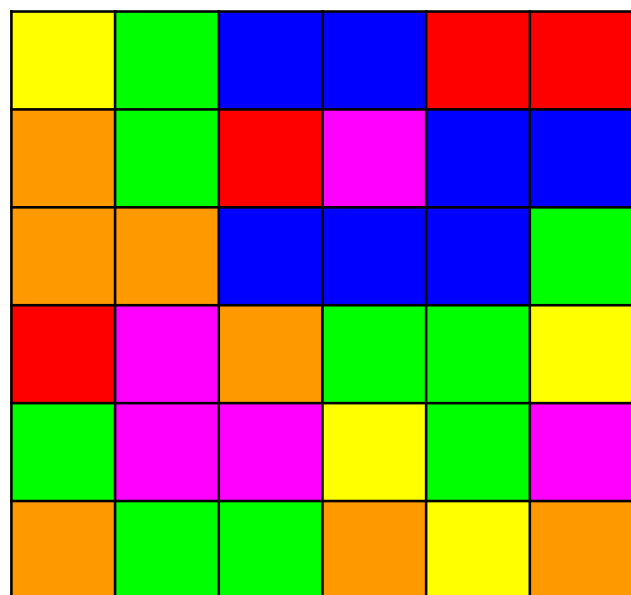
内存约束难题



比特币前就存在  
加密个人口令

2009

反ASIC



检验成本过高

内存使用参数  
设置过低

组合多种Hash算法

XII

参数

反ASIC是否可能

SHA256

反ASIC是否有问题



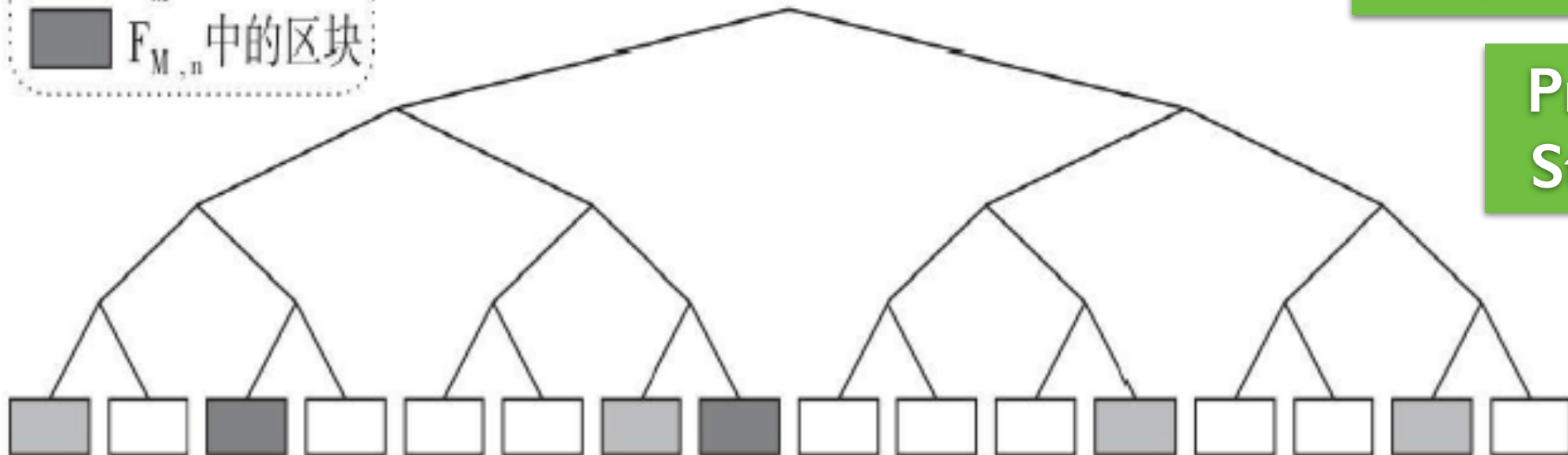
# 有效工作量证明

挖矿能量消耗问题

志愿者计算项目



F 的根

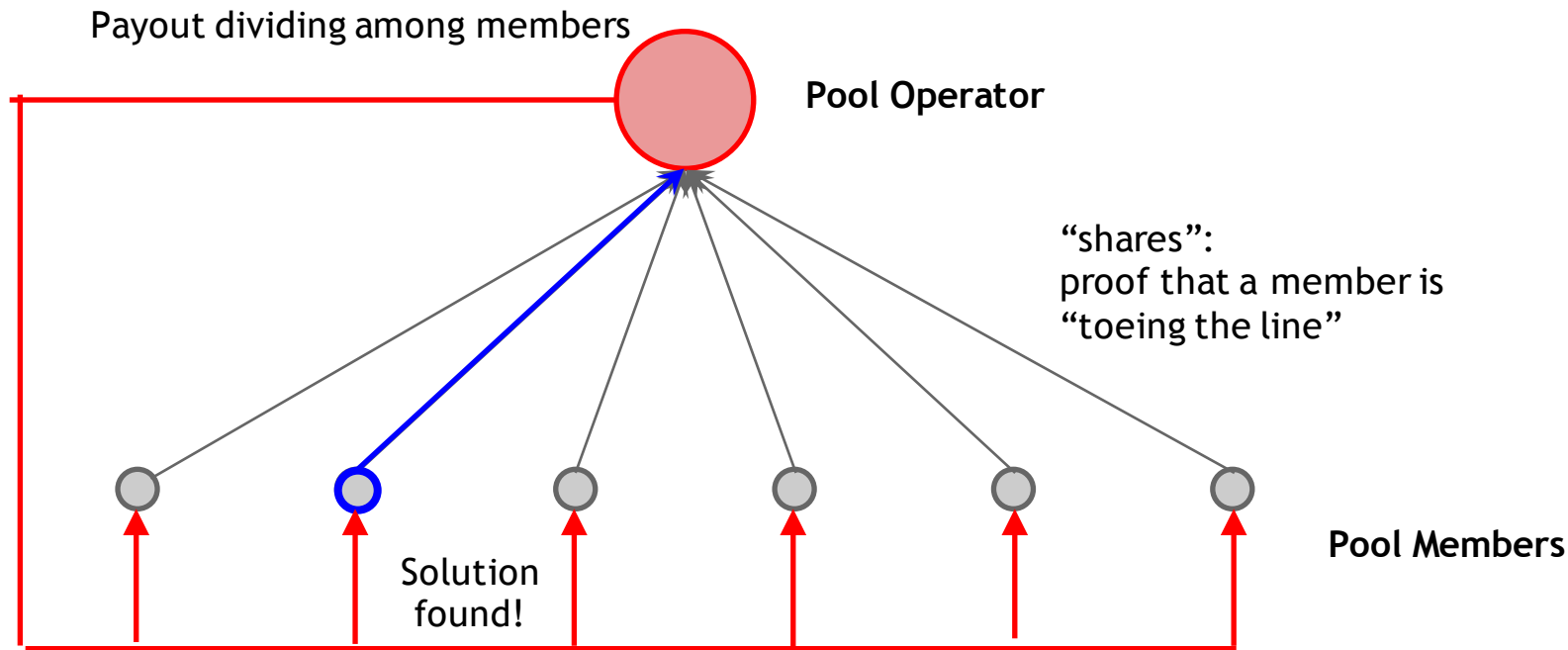


存储量证明

Proof of Storage

分布式  
存储

# 不可外包的难题



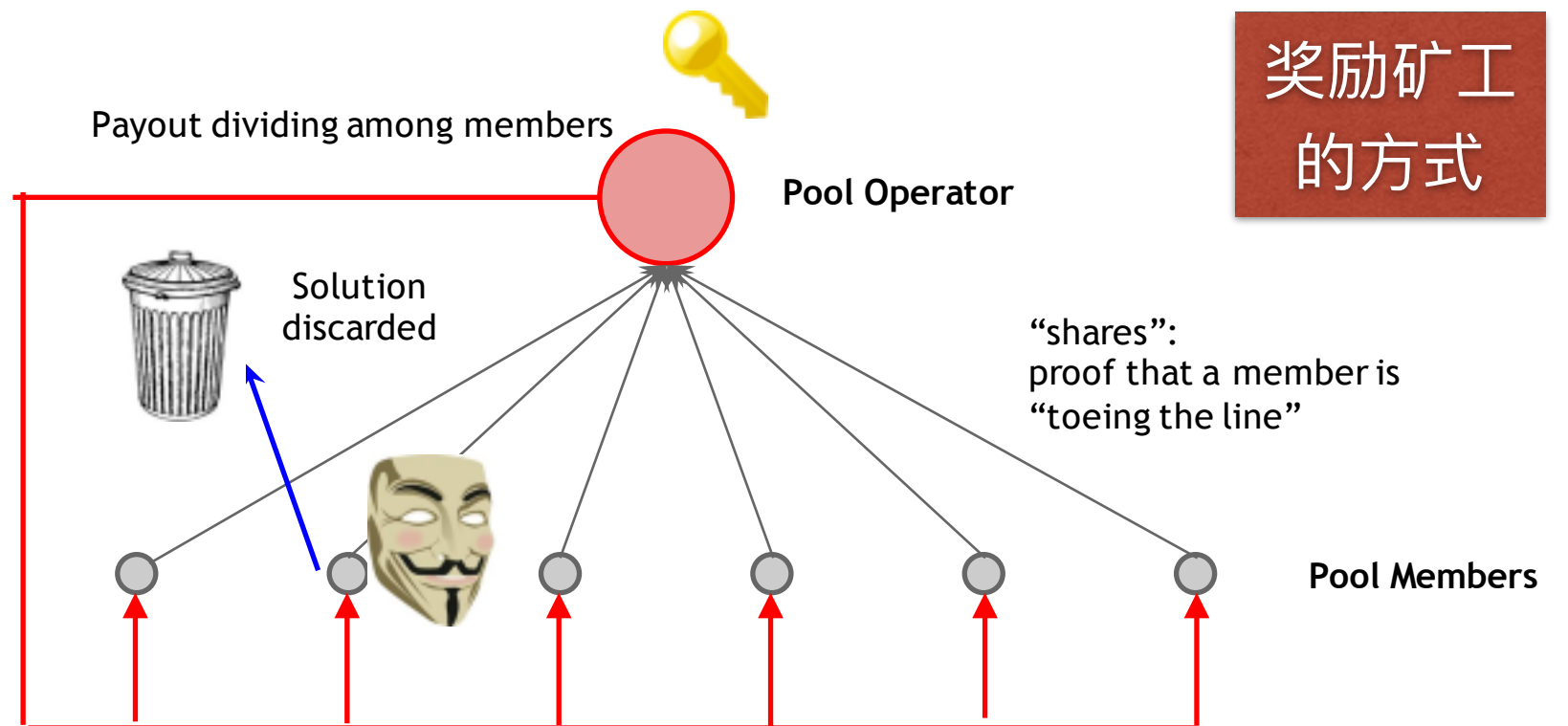
防止矿池的产生

中心化、安全

区块丢弃攻击

奖励破坏

区块数字签名的哈希值  
低于一个特定的目标



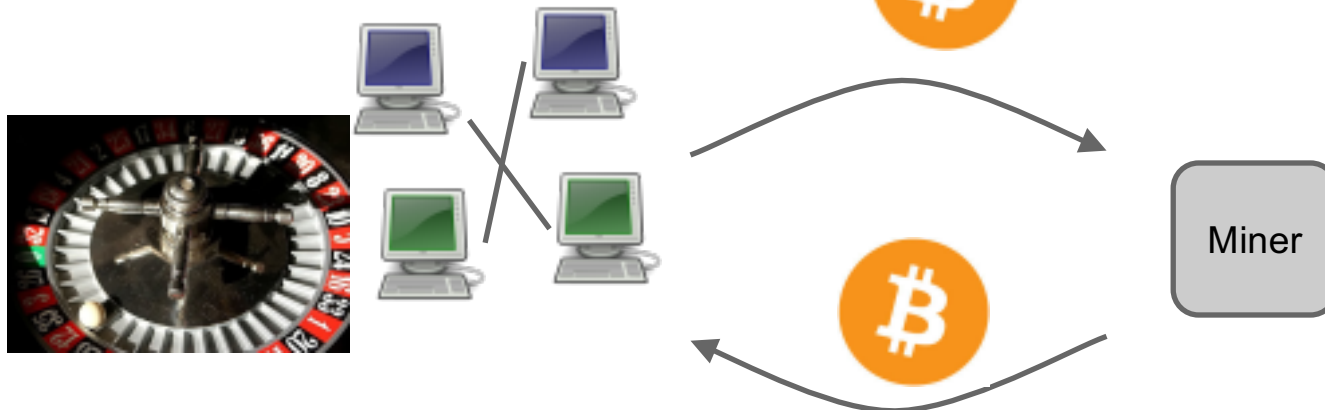
奖励矿工  
的方式



权益证明

分叉攻击

检查点

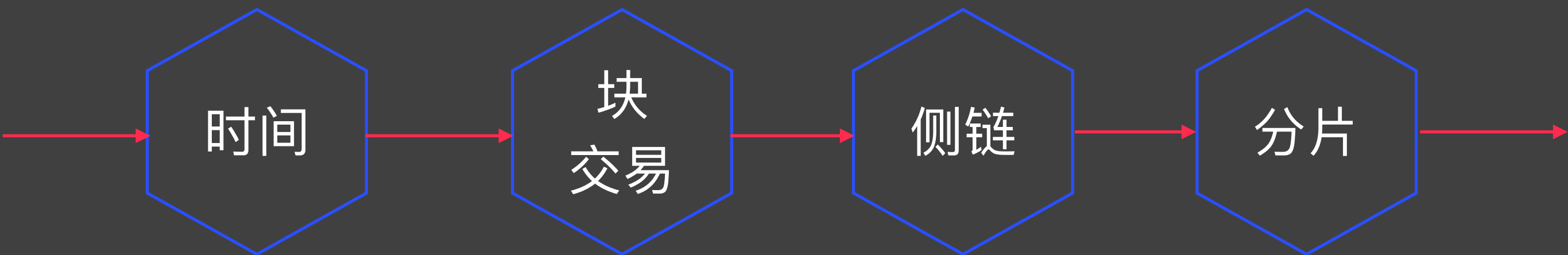


2012

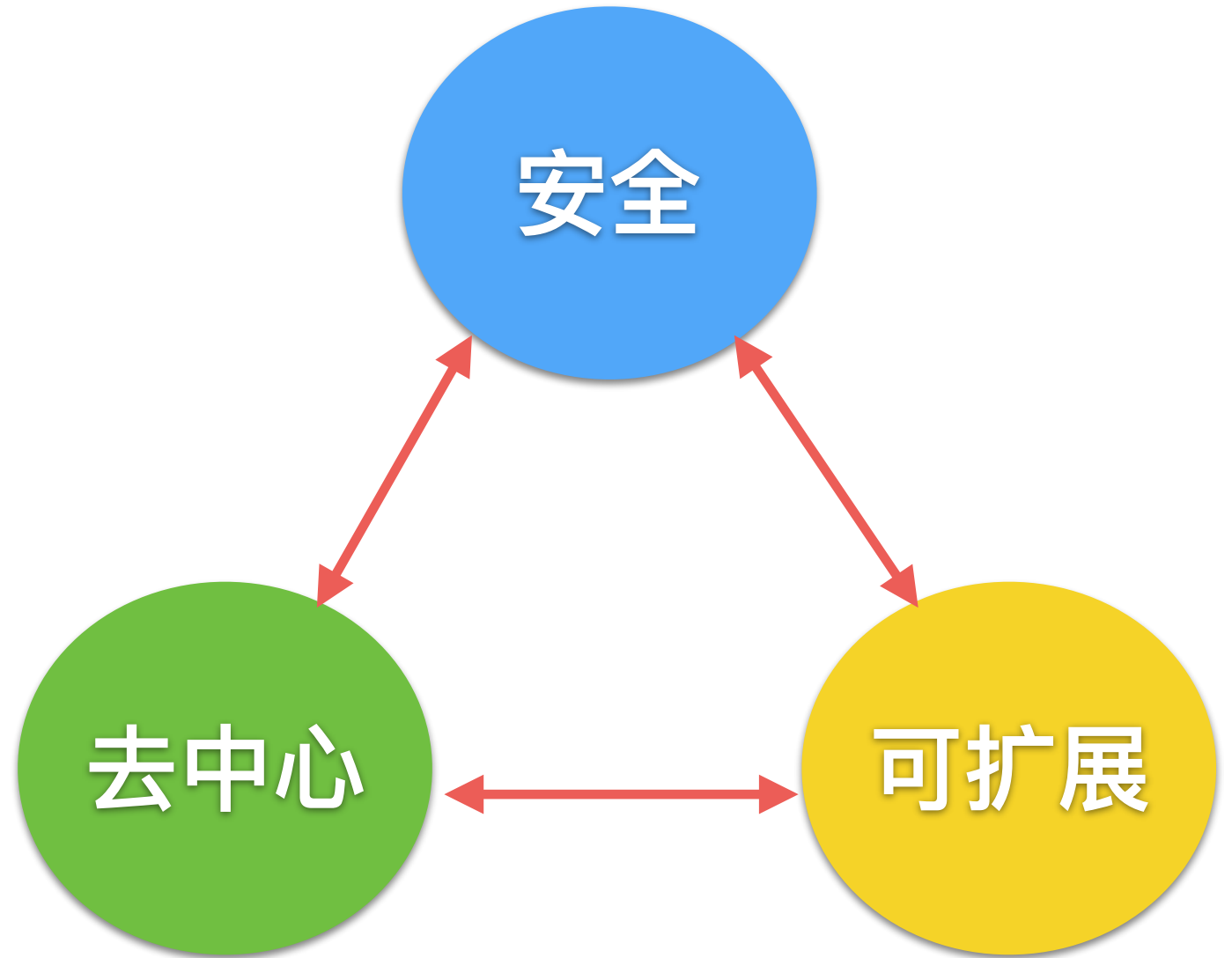
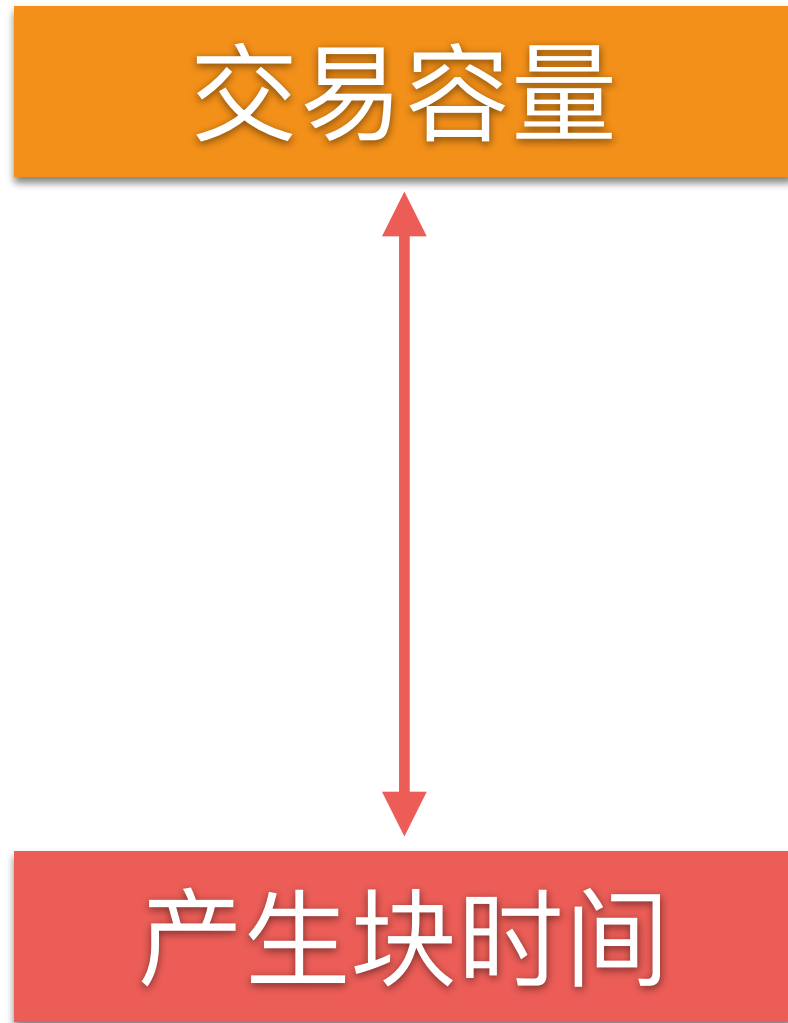
点点币

币拥有量  
交易

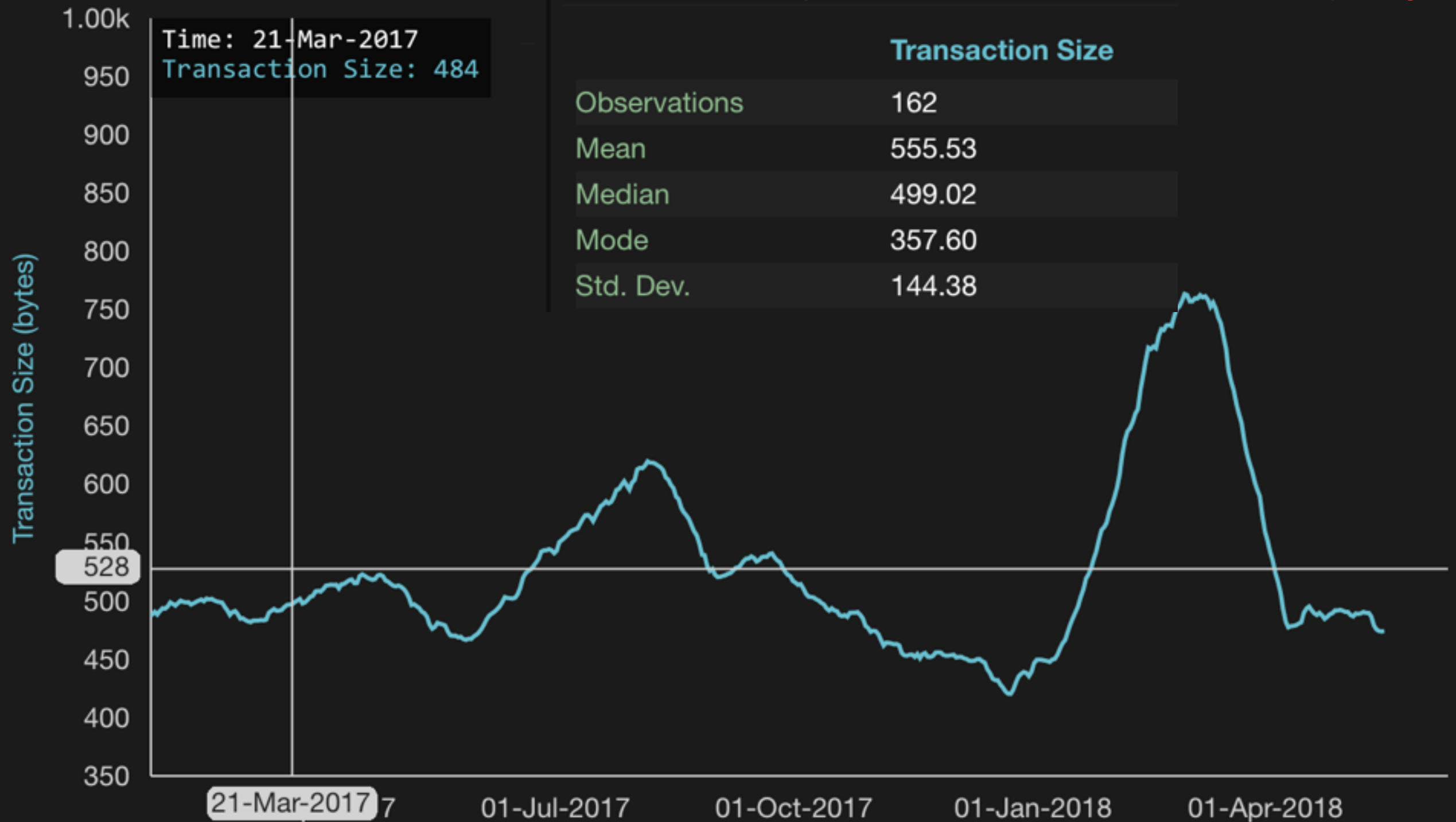
# 可扩展性







[https://tradeblock.com/bitcoin/historical/1d-f-tsize\\_per\\_avg-00271](https://tradeblock.com/bitcoin/historical/1d-f-tsize_per_avg-00271)



# 没有比较没有伤害



3

3.2



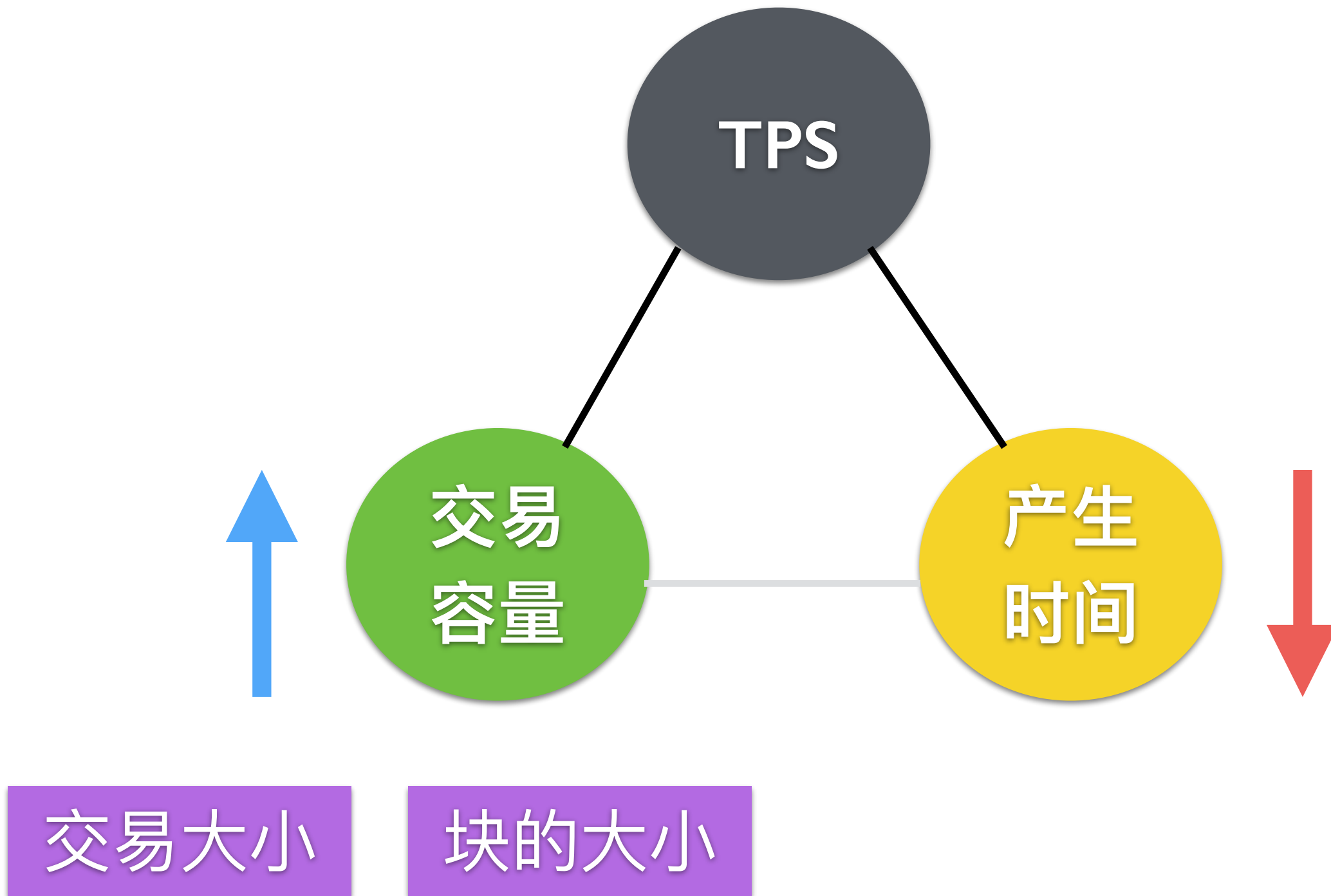
150

450



2000

56000



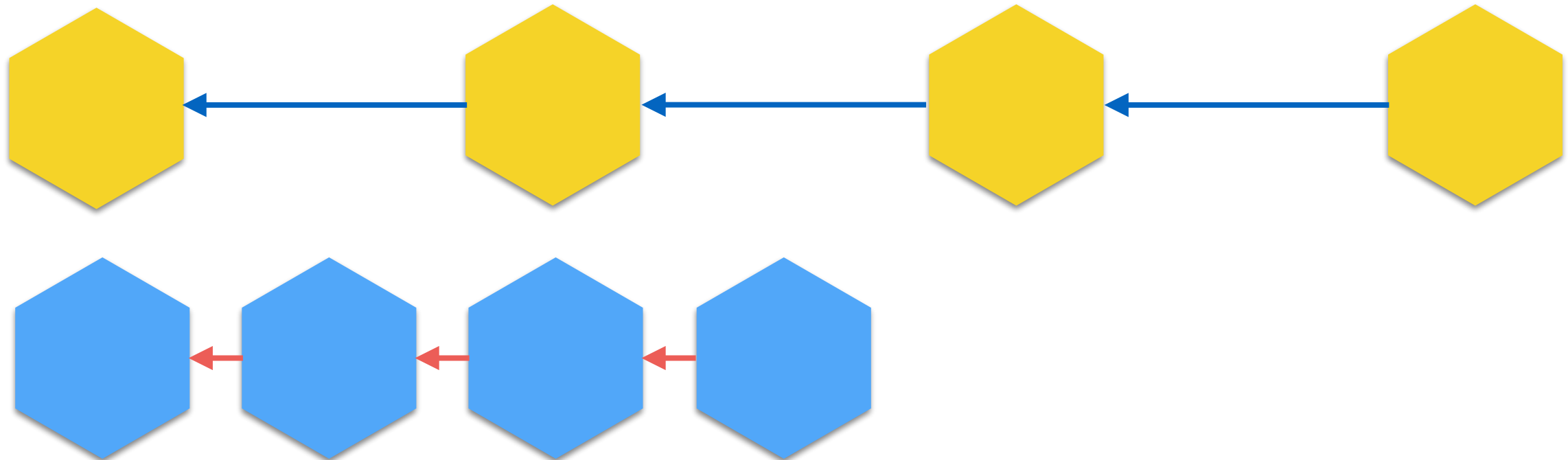
# 减少块产生时间

块传播时间

块产生时间

块传播时间

块产生时间

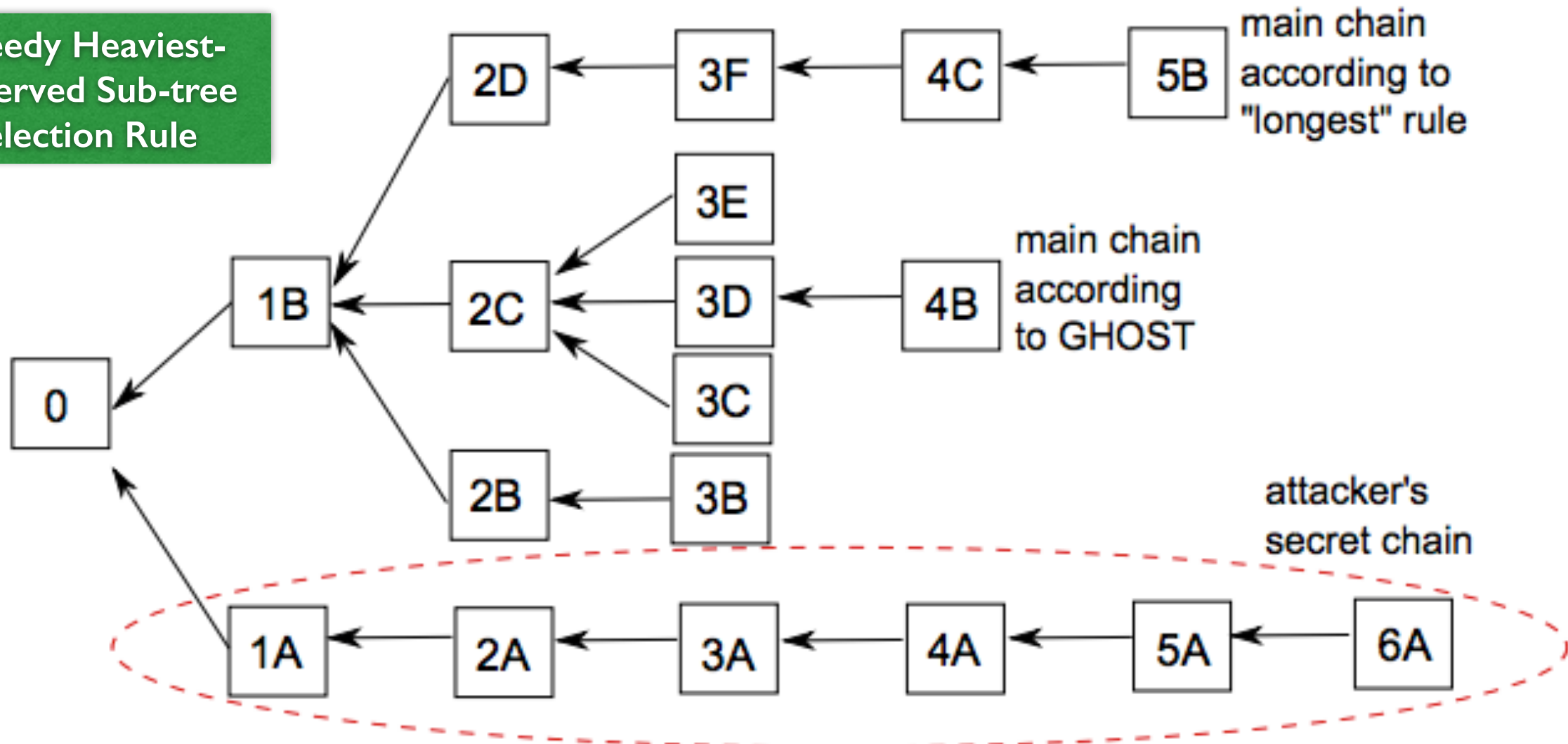




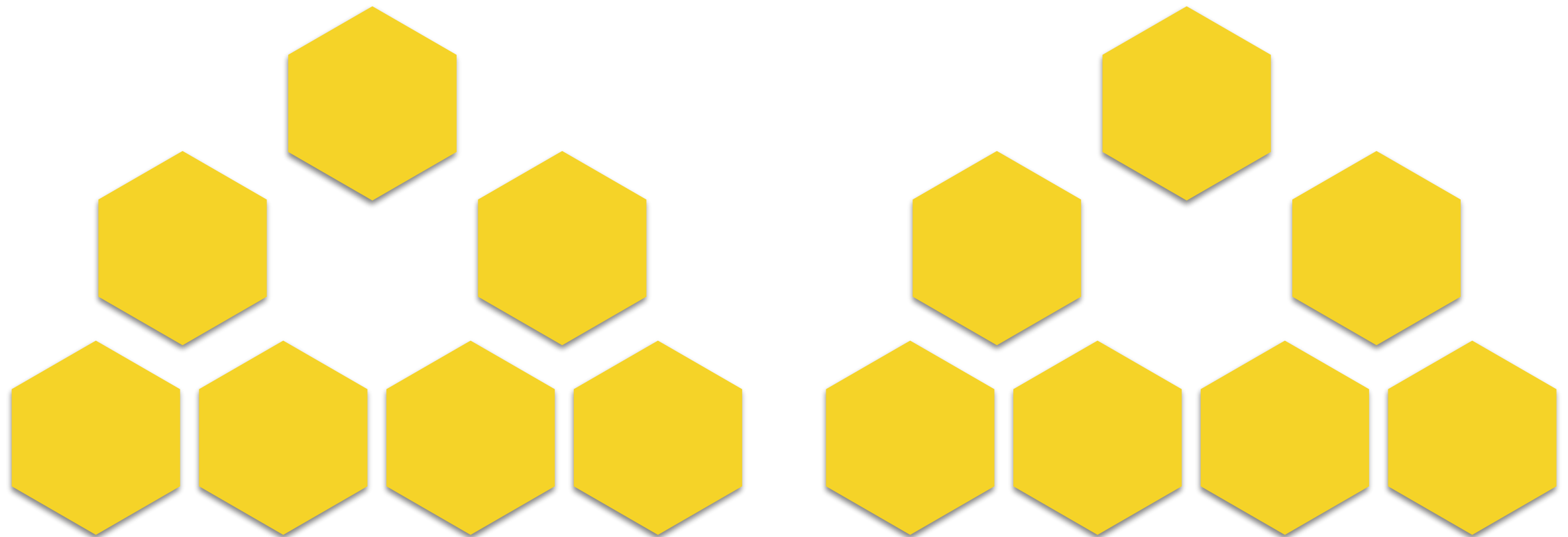
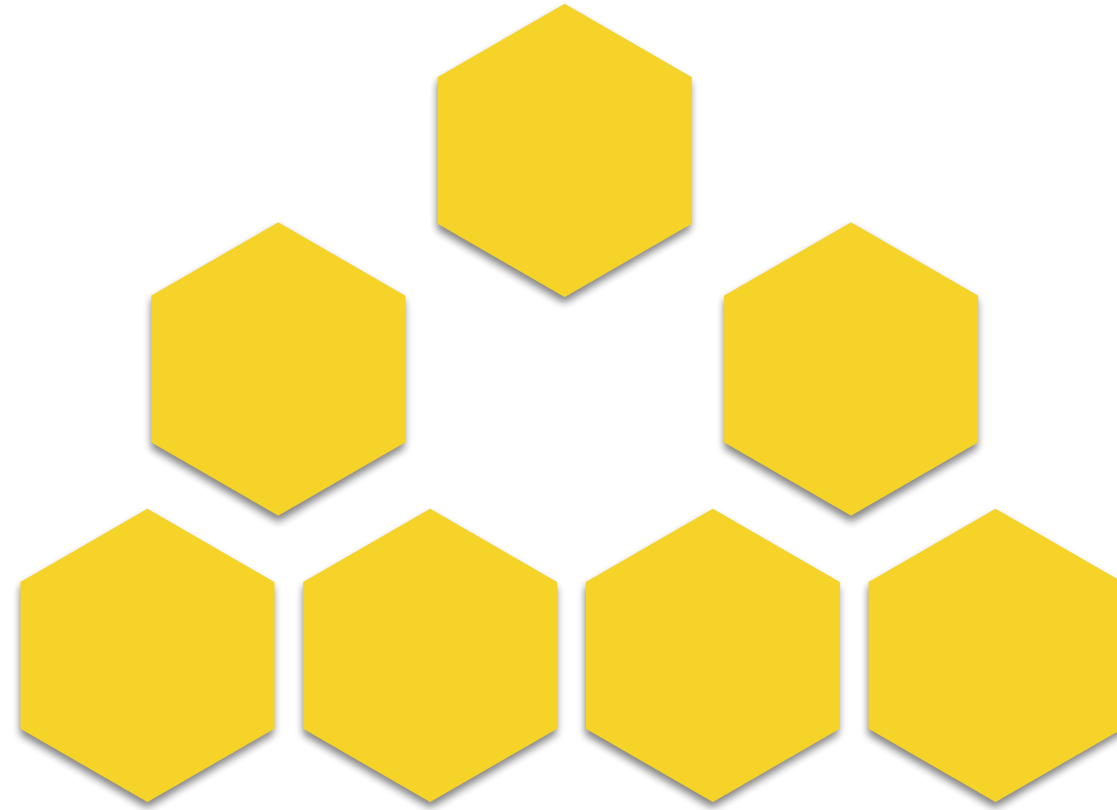
## Secure High-Rate Transaction Processing in Bitcoin

Financial Cryptography and Data Security 2015

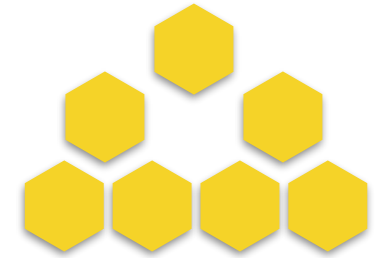
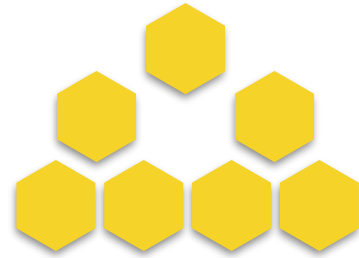
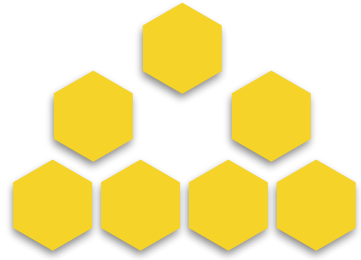
Greedy Heaviest-  
Observed Sub-tree  
selection Rule



# 增大块大小



# 增大块大小



容易执行

更低的成本

矿工同意即可

硬分叉

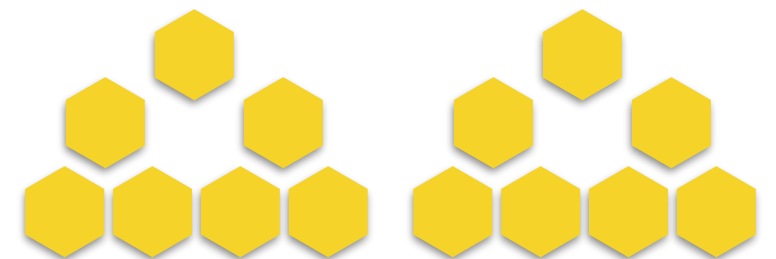
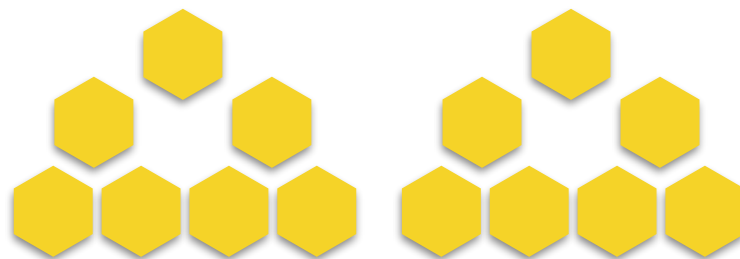
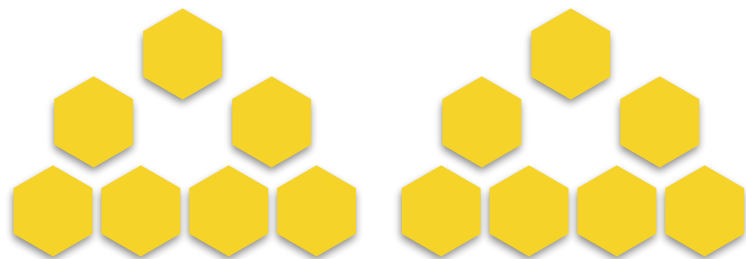
计算能力

更长的传播时间

大小增长块

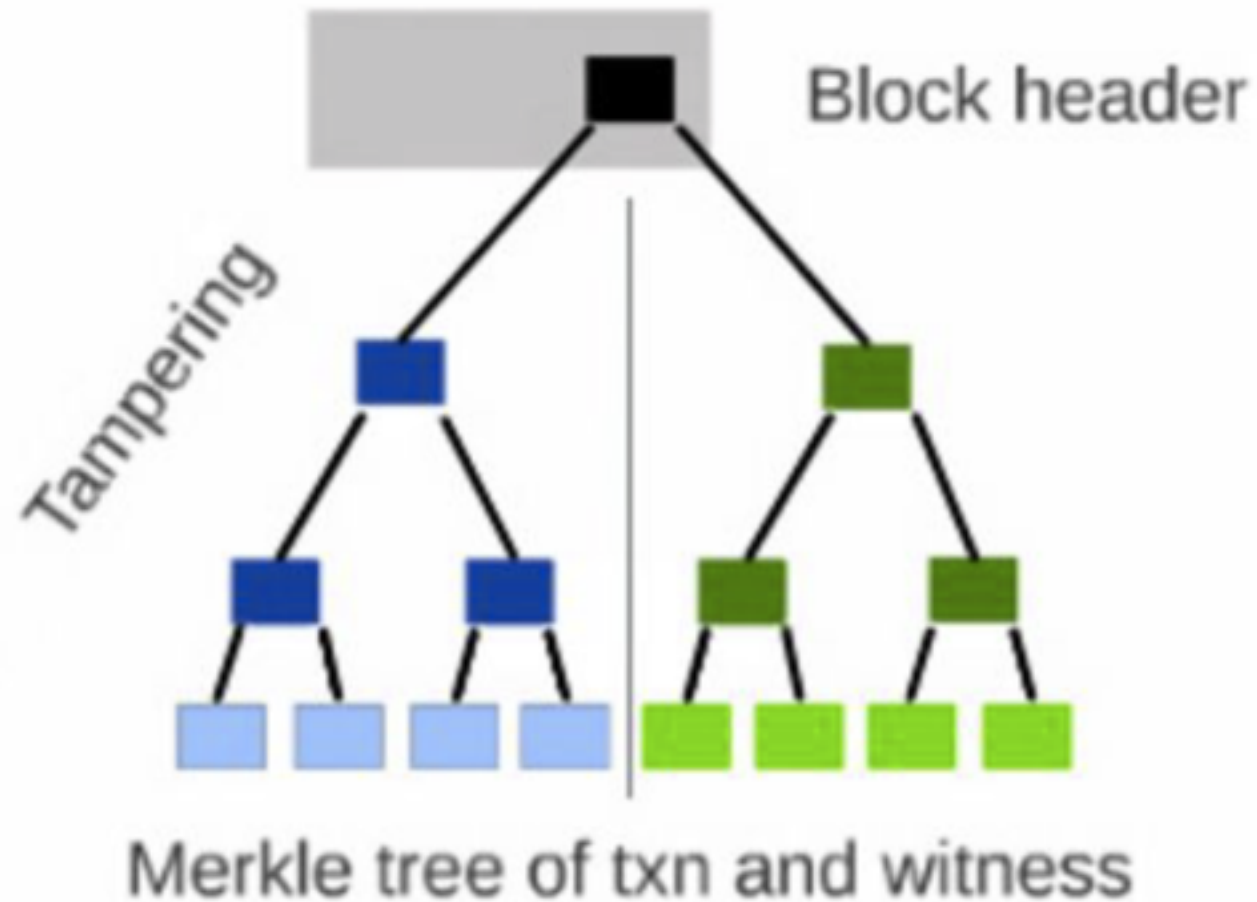
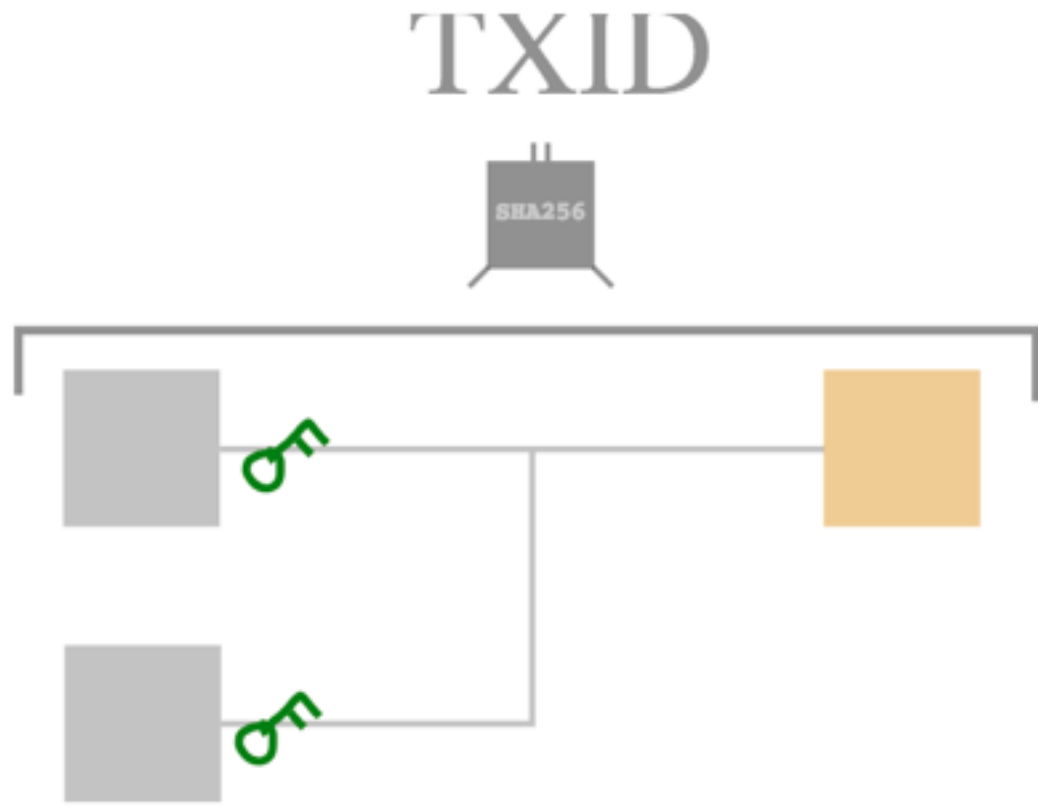
挖矿设备

安全性



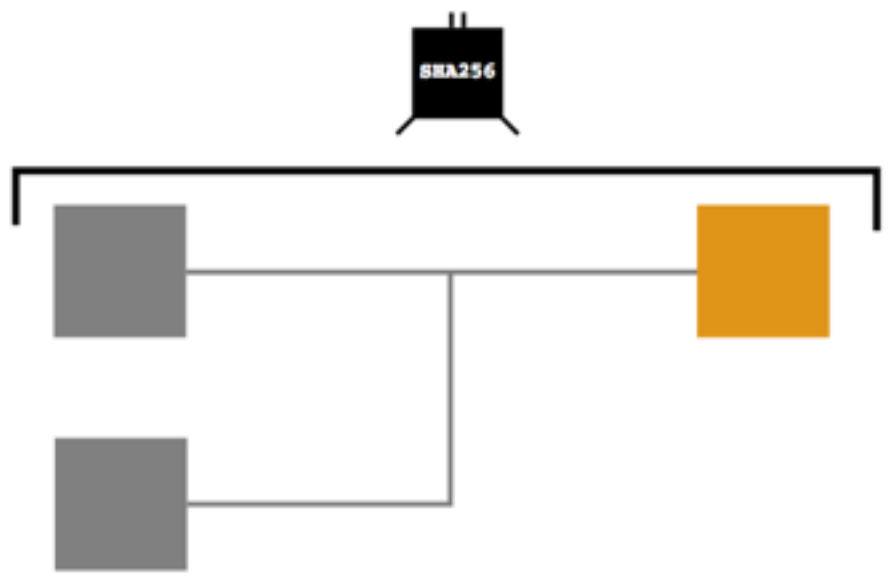
# 减少交易大小

<http://learnmeabitcoin.com/faq/segregated-witness>



TXID

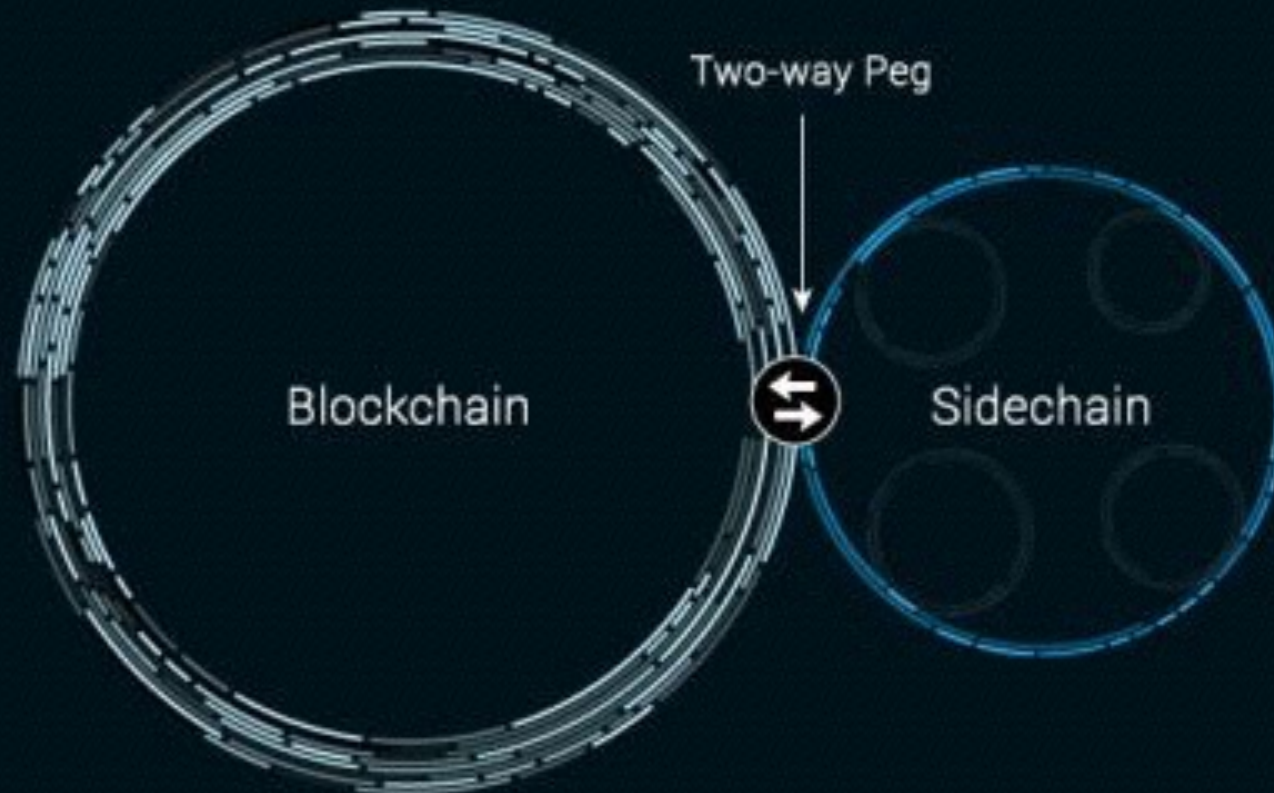
隔离  
见证



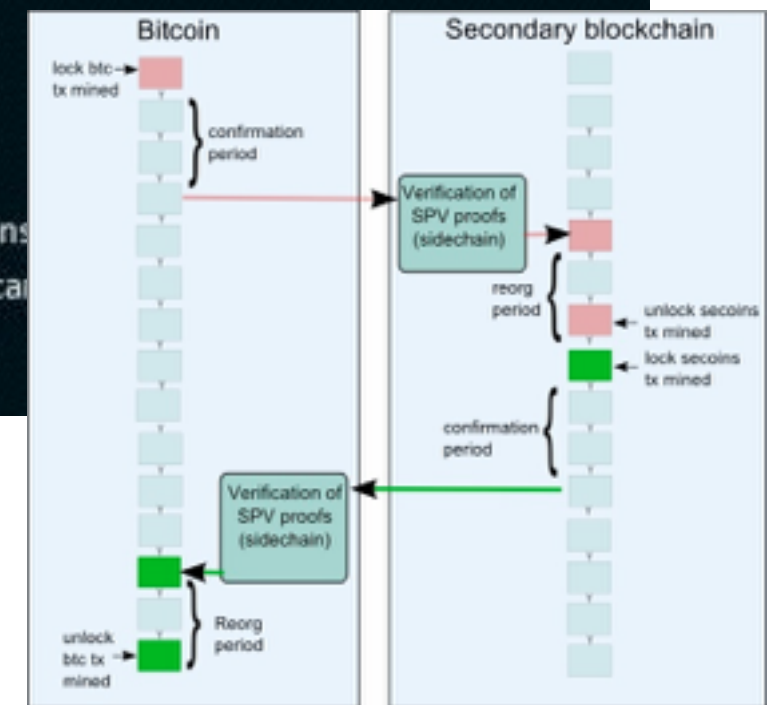
Segregated Witness

优点

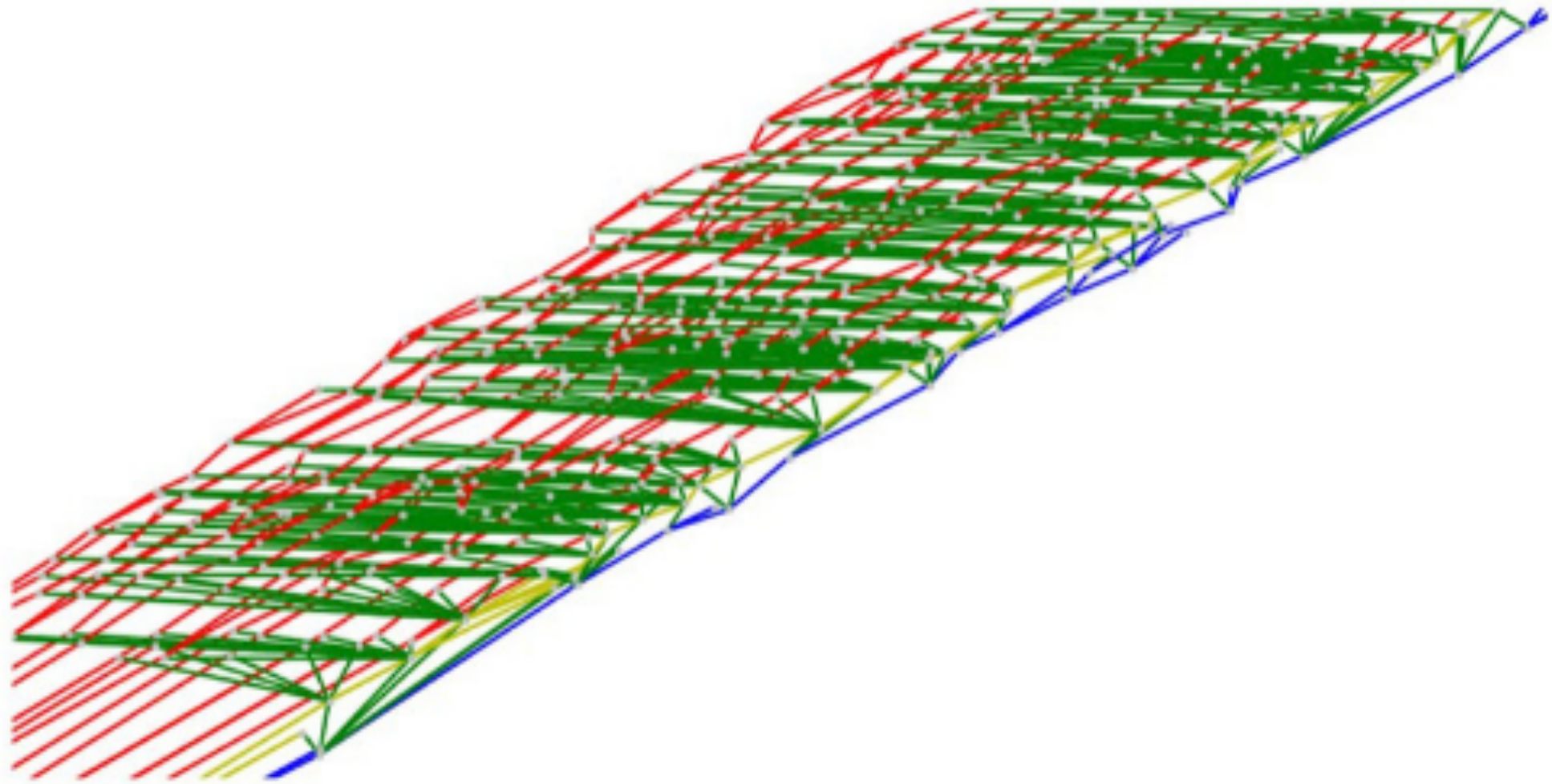
缺点



The use of a **two-way peg** enables coins or other assets to be transferred between chains at an otherwise deterministic exchange rate. A pegged sidechain is a sidechain whose assets can be transferred from and returned to other sidechains.

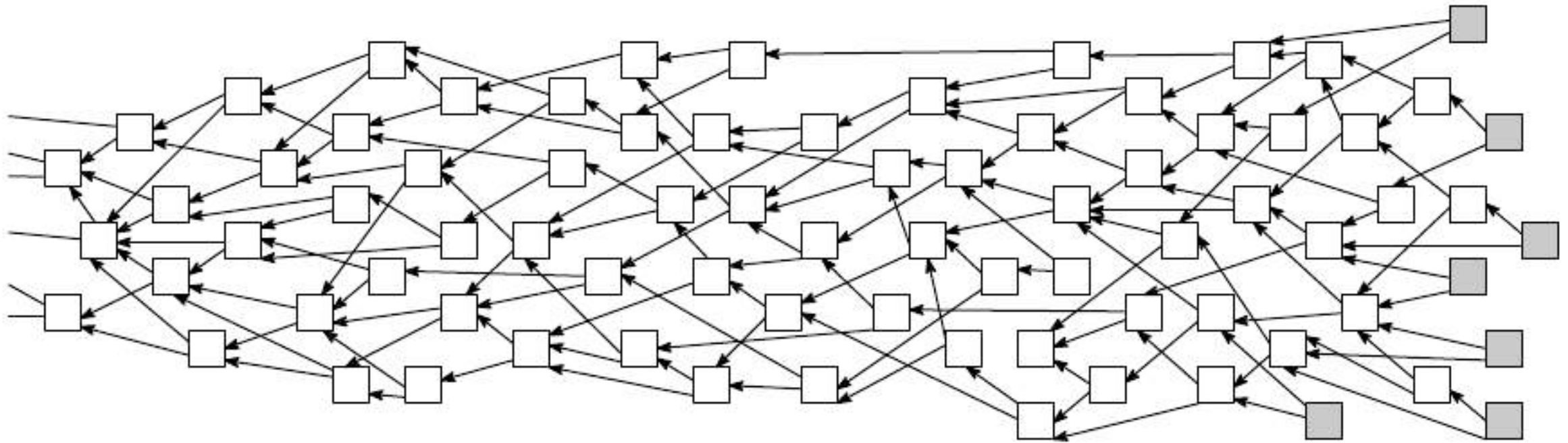








# DAG



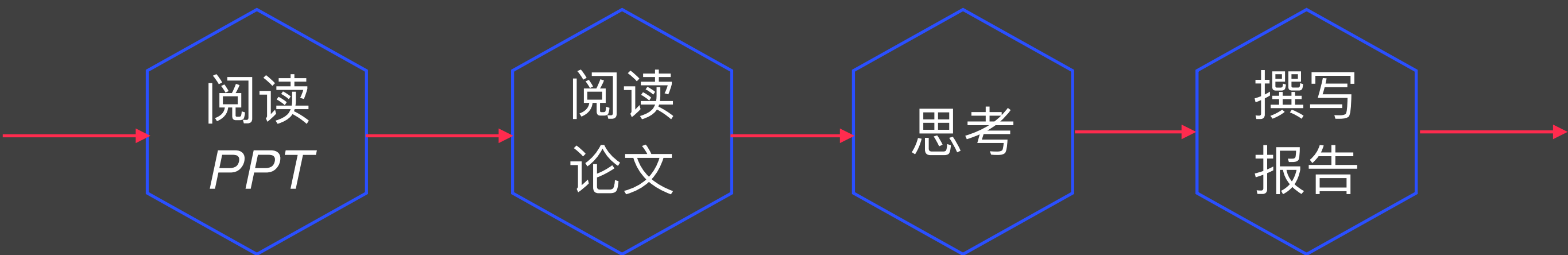
# 课后作业

阅读  
*PPT*

阅读  
论文

思考

撰写  
报告



要求阅读如下论文，写阅读报告

## Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains

Elli Androulaki  
Artem Barger  
Vita Bortnikov  
IBM

Christian Cachin  
Konstantinos Christidis  
Angelo De Caro  
David Enyeart  
IBM

Christopher Ferris  
Gennady Laventman  
Yacov Manevich  
IBM

*In EuroSys 2018.*

- 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](mailto:sunhp@ss.pku.edu.cn)*

*<https://huipingsun.github.io>*