区块链技术 II

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

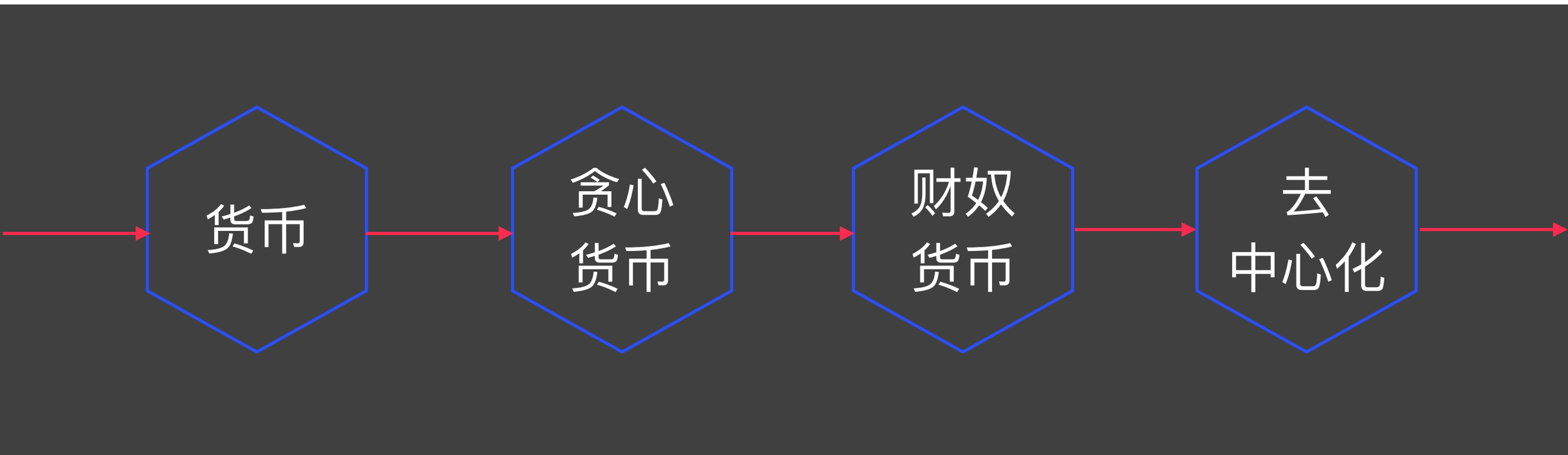
Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

Course Overview

上次课程内容

1 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

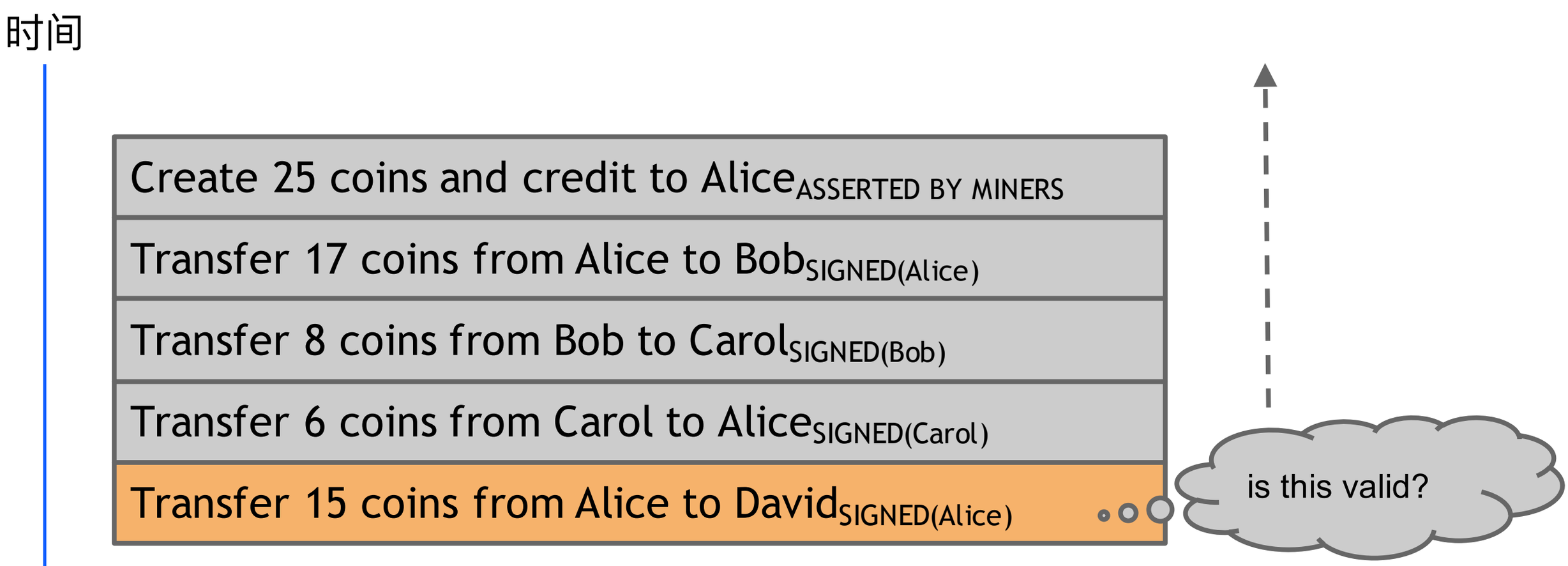
加密货币



货币


新版
2015年版 第5套
人民币
那些事...
中国人民银行
100
壹佰圆
样币
AA00000000
钞票正面
钞票背面
ZHONGGUO RENMIN YINHANG
100
YUAN
2015年
样币禁止流通
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。
光变镂空开窗安全线
胶印凹印
胶印对印图案
光彩光变数字
白水印
人像水印
镂空双号码
广发银行
CGB

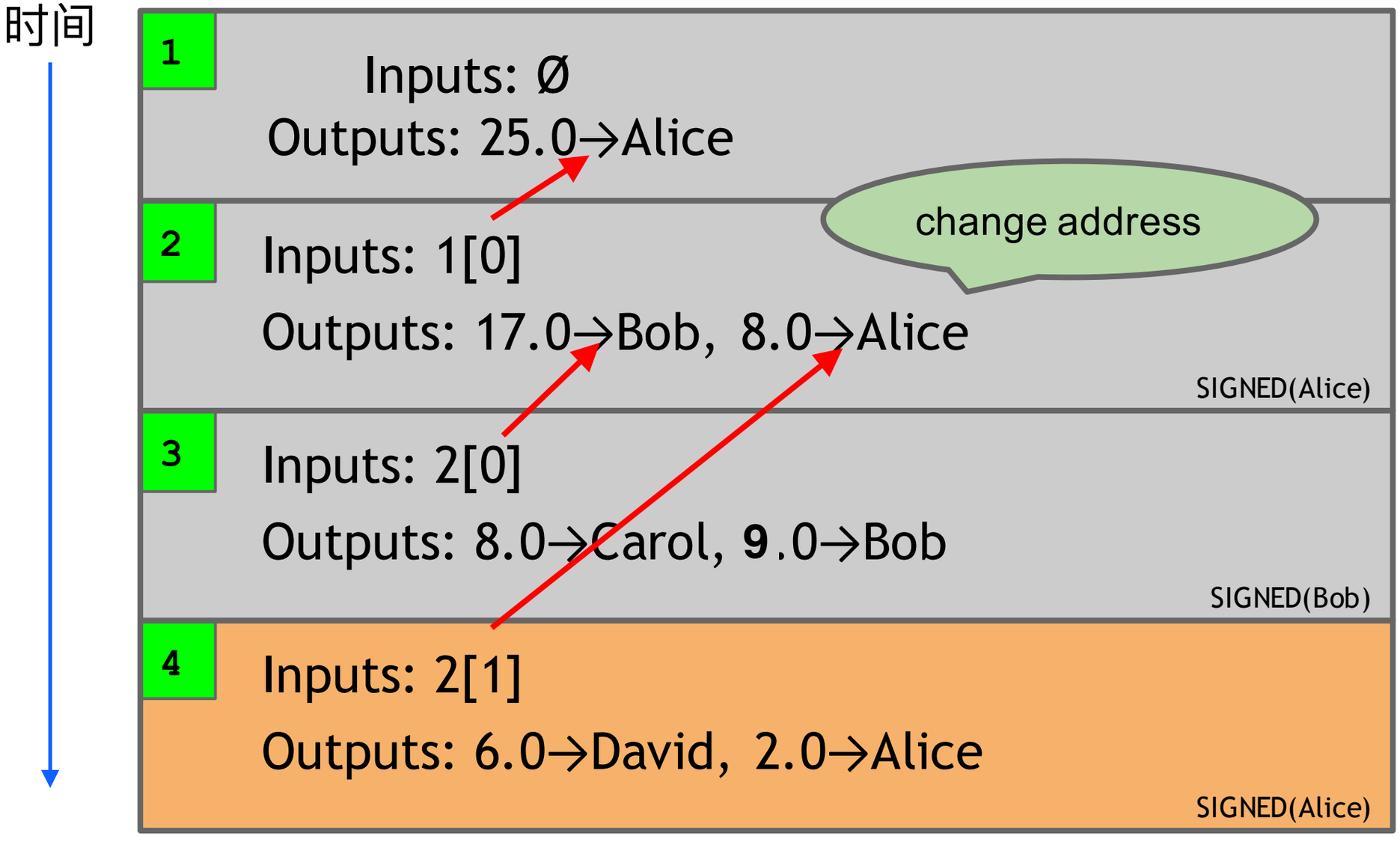
普通账本



一个块包含一个交易

交易验证需要扫描以前所有的块

采用区块链



we implement this with hash pointers

finite scan to check for validity

is this valid?

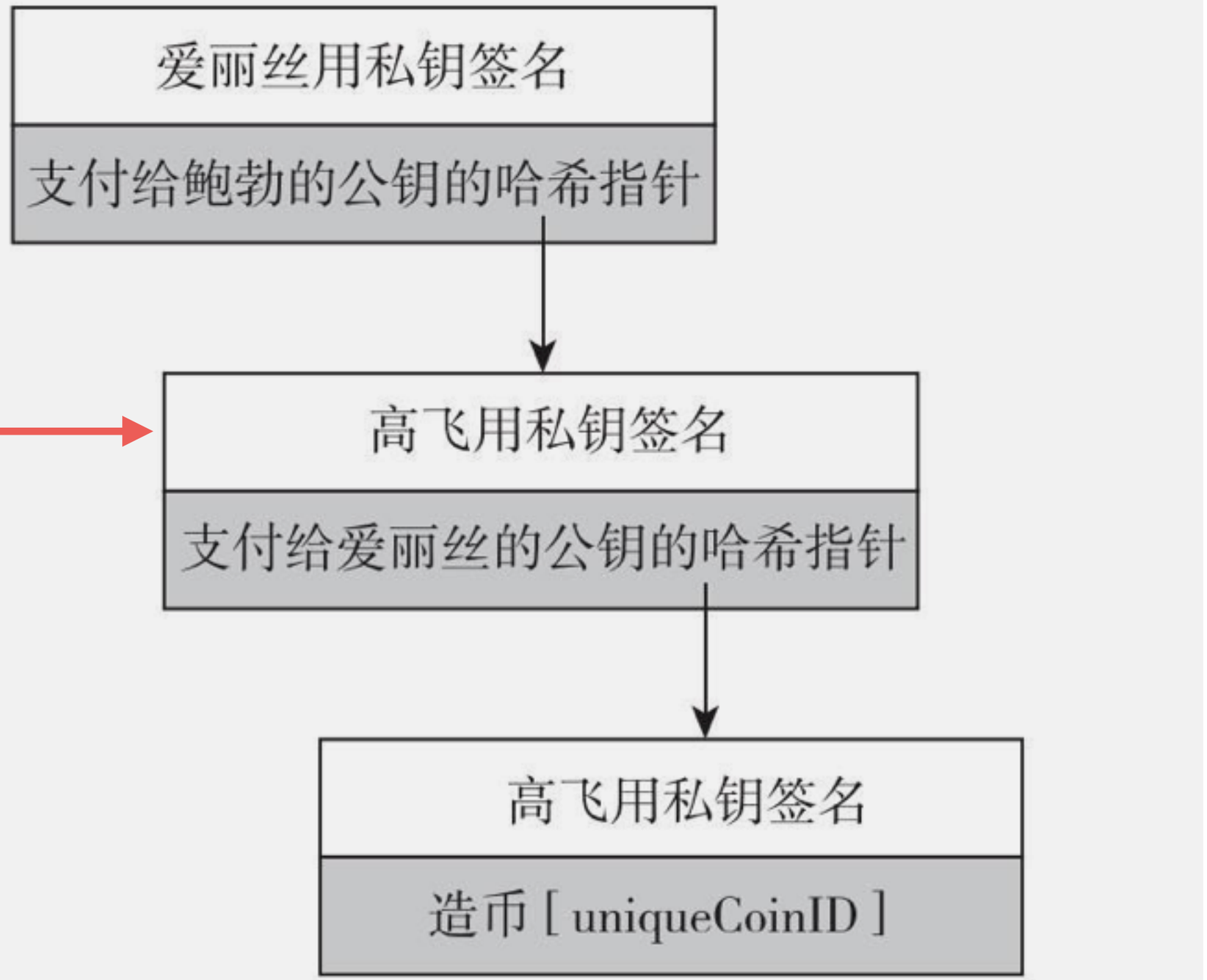
一个块包含一个交易

交易验证需要扫描以前所有的相关块

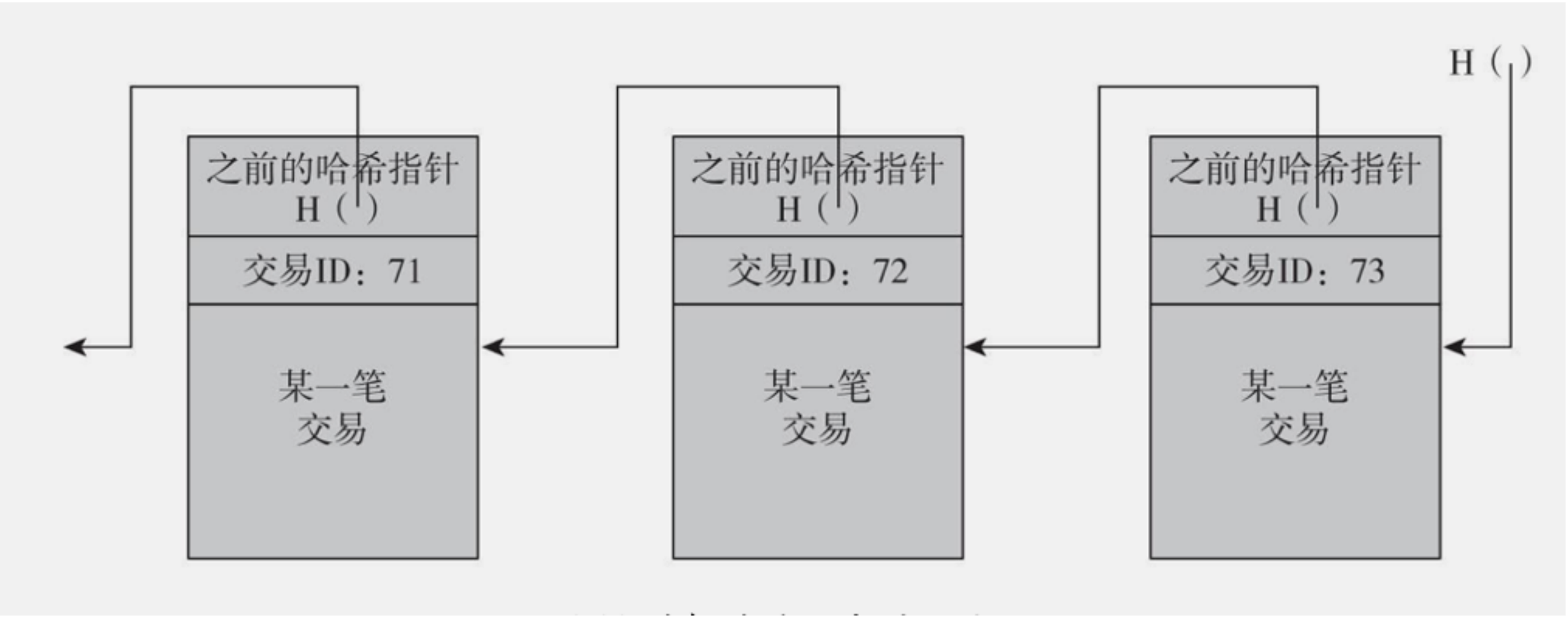
高飞币

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

比特币如何实现去中心

- 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? 技术

- 谁决定系统如何改变规则? 激励
- 比特币如何获得交易价格

用户:对等网络 矿工 挖矿 开发人员:软件更新

恶意节点

窃取比特币

拒绝服务攻击

双重支付攻击

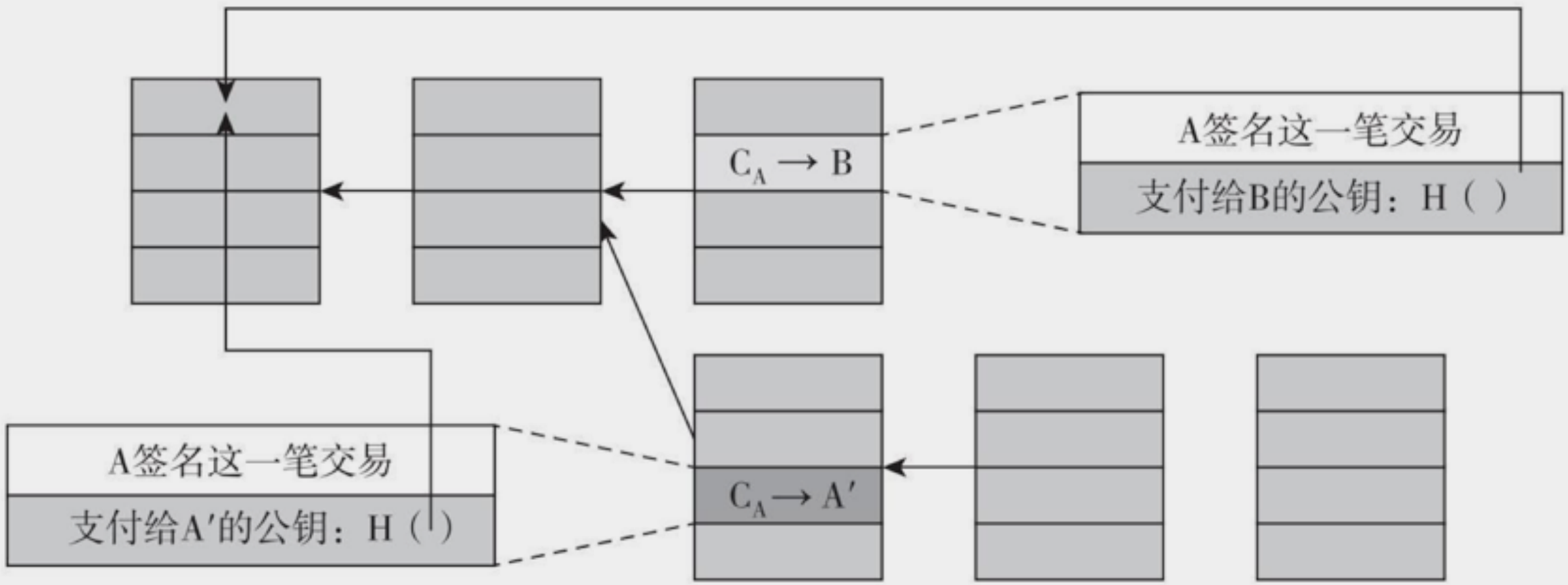


图2.2 双重支付攻击

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

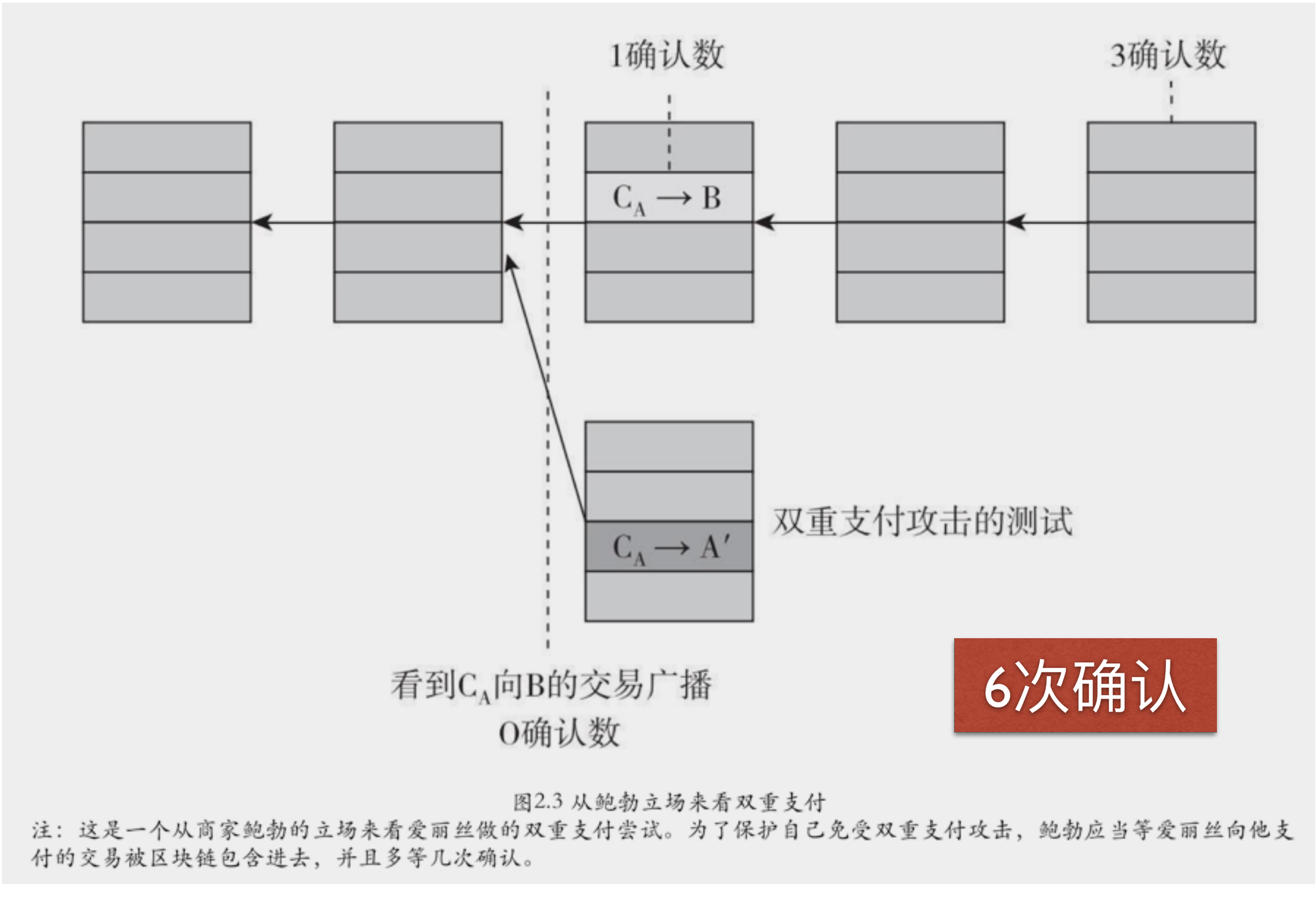
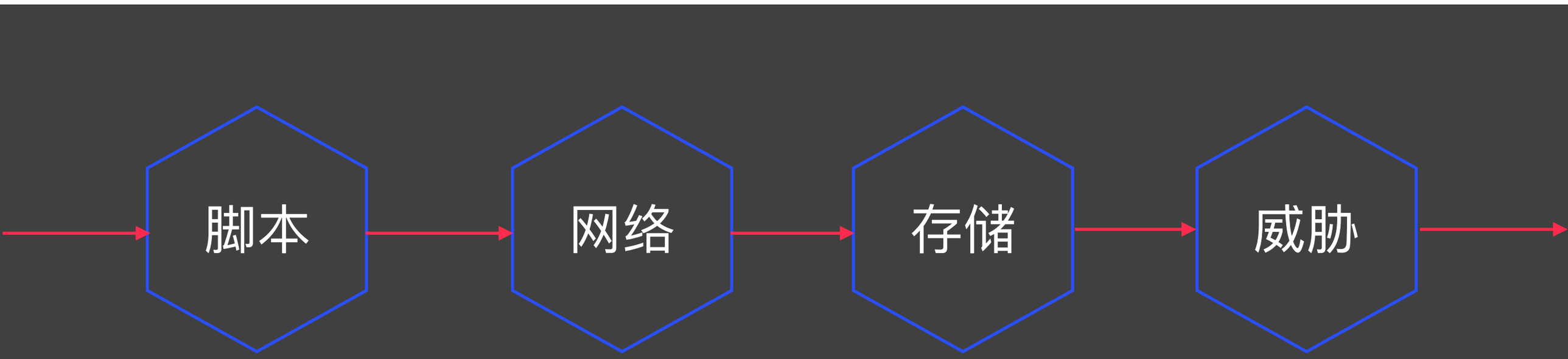


图2.3 从鲍勃立场来看双重支付

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



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
```

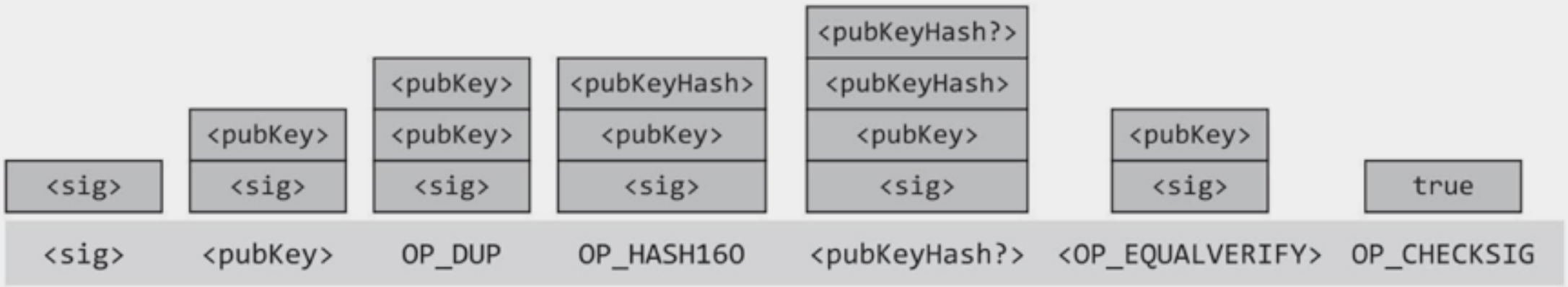
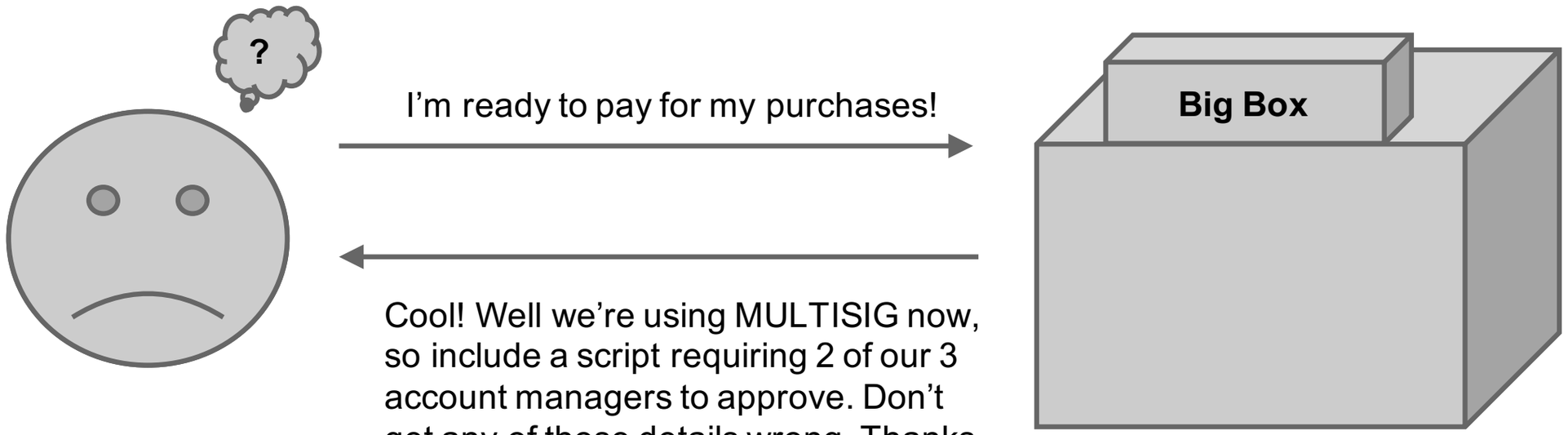
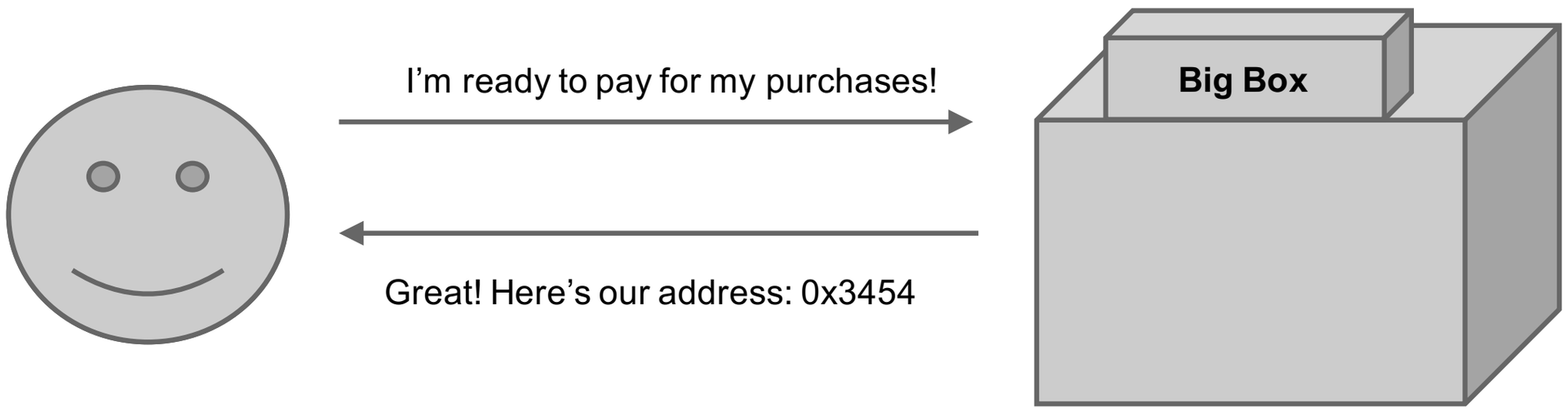


图3.6 比特币脚本的执行堆栈状态图

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!
Big Box
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!
Big Box
Great! Here's our address: 0x3454

比特币交易程序

元数据

```
{
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
```

输入

```
  "in":[
   {
      "prev_out":{
      "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
      "n":0
     },
       "scriptSig":"30440..."
   },
   {
      "prev_out":{
      "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
      "n":0
     },
     "scriptSig":"3f3a4..."
   }
  ],
```

输出

```
  "out":[
   {
     "value":"10.12287097",
     "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e
            OP_EQUALVERIFY OP_CHECKSIG"
   }
  ]
}
```

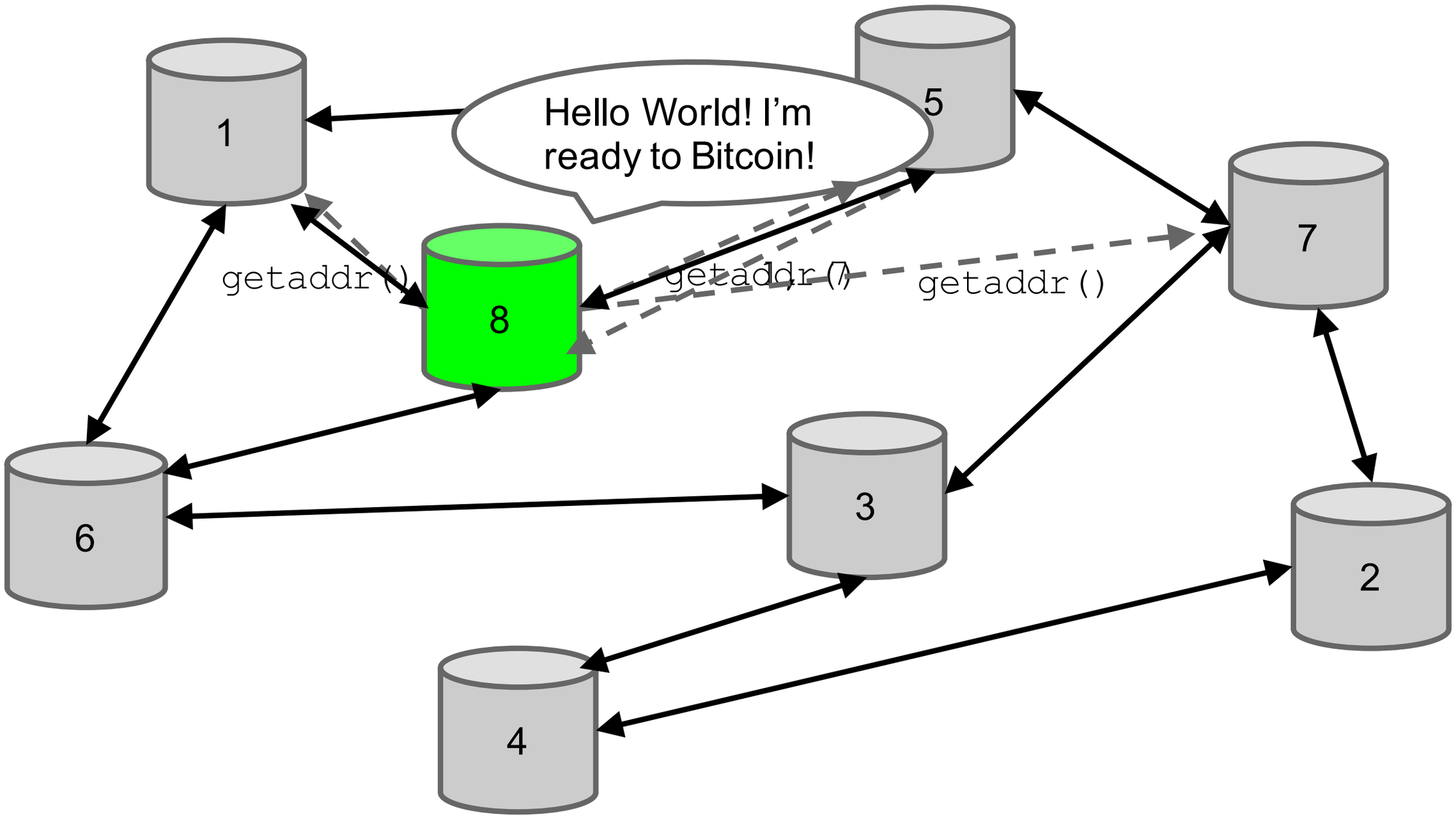
图3.3 一个真实的比特币交易程序段

币基交易

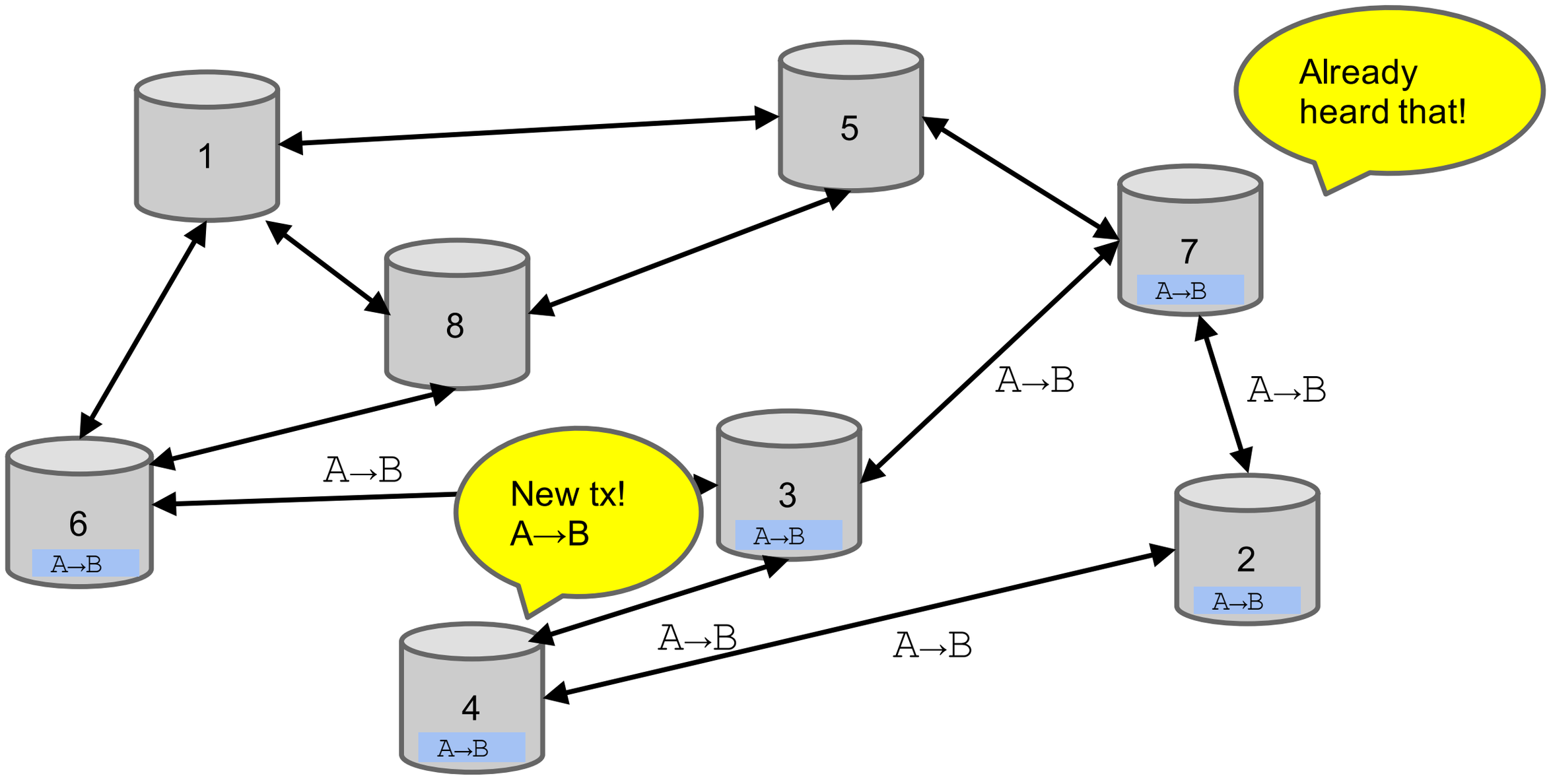
```
"in":[
        {
          "prev_out":{
            "hash":“000000.....0000000",
            "n":4294967295
          },
           "coinbase":"..."
      },
      [
  "out":[
        {
          "value":"25.03371419",
          "scriptPubKey":"OPDUP OPHASH160 ... ”
        }
       ]
```

图3.8 币基交易

比特币网络


1
Hello World! I'm
ready to Bitcoin!
5
getaddr()
8
getaddr()
getaddr()
7
6
3
2
4

比特币网络交易消息传播



块传播

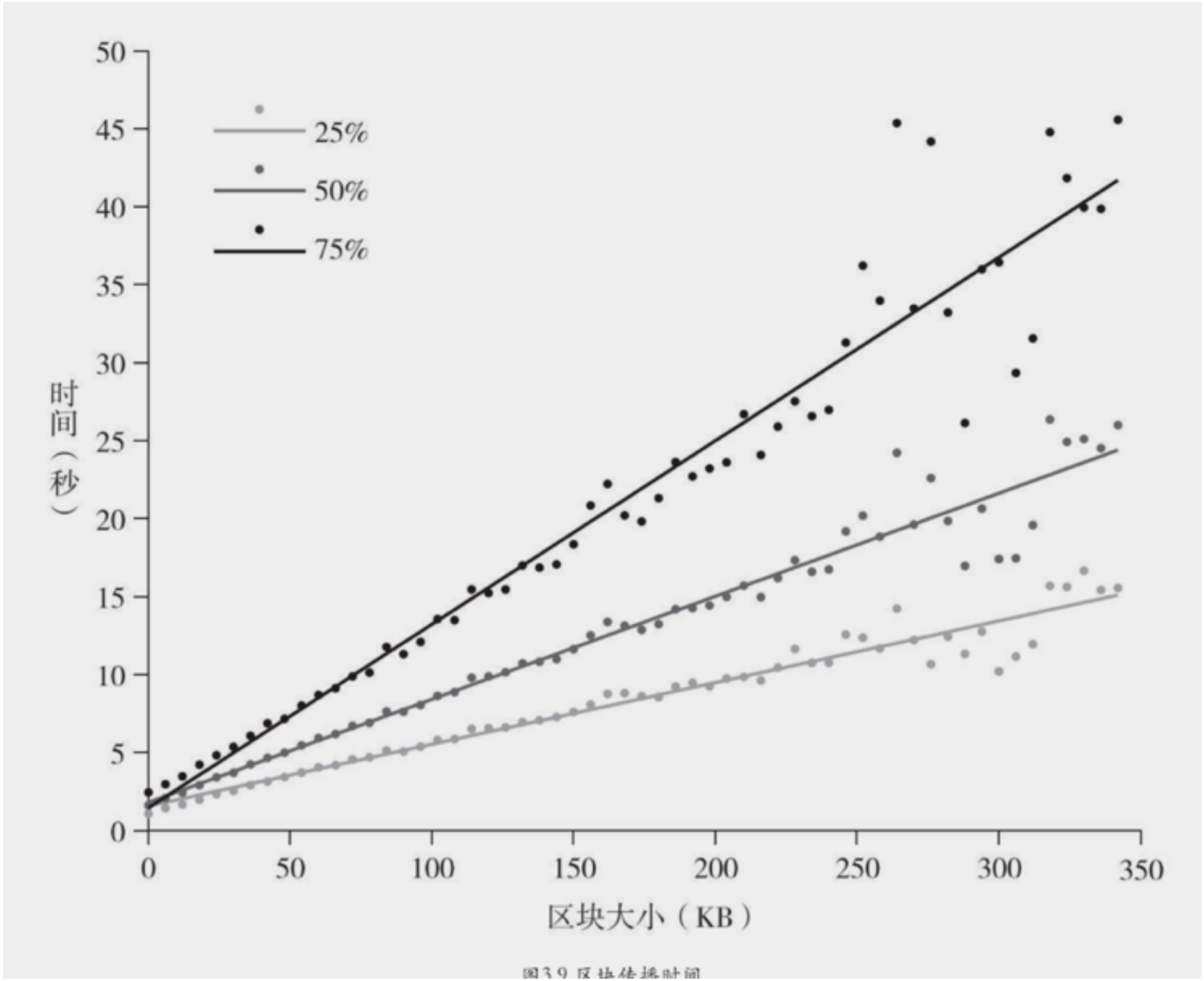


图3.9 区块传播时间

存储花费

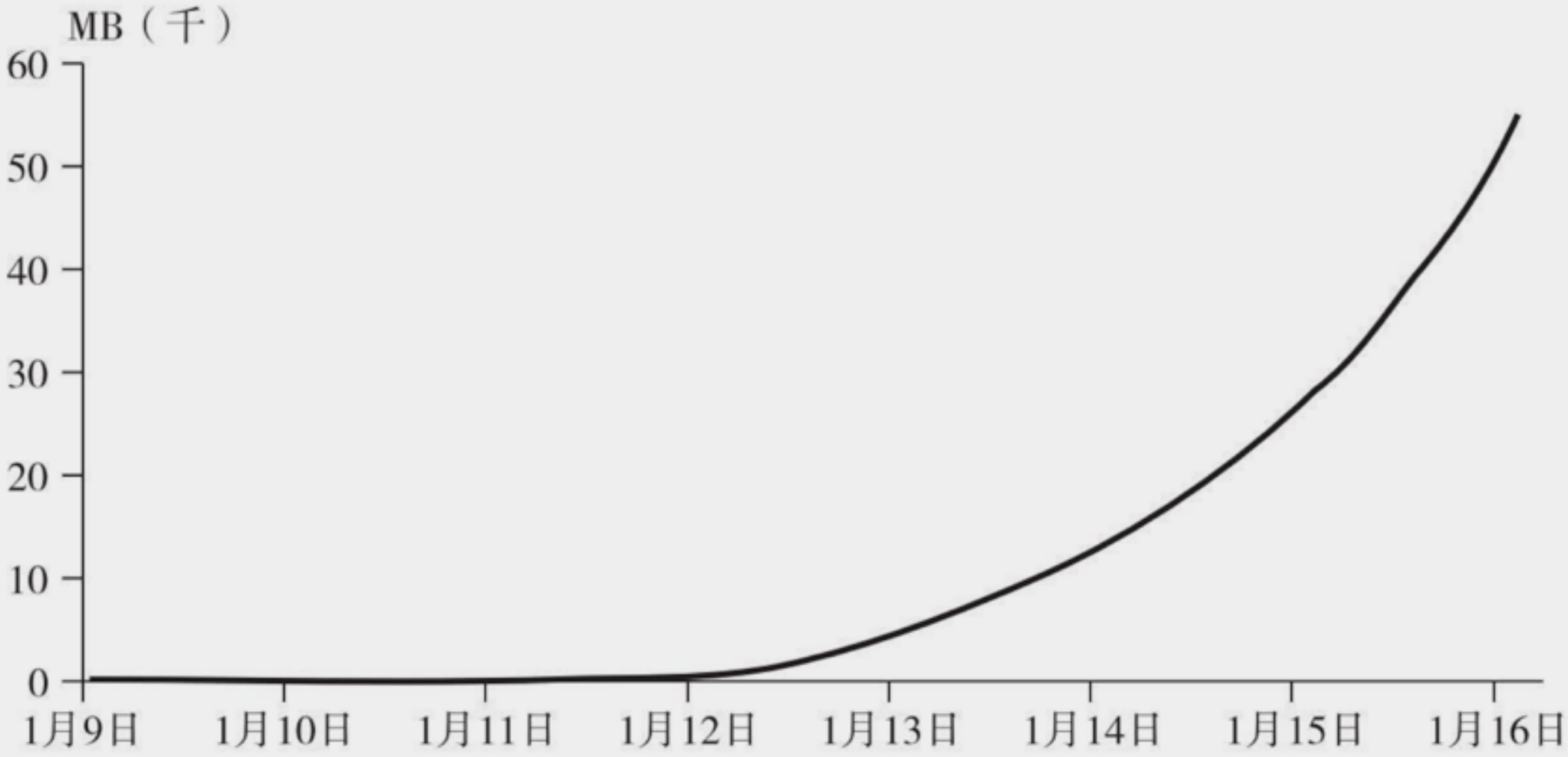
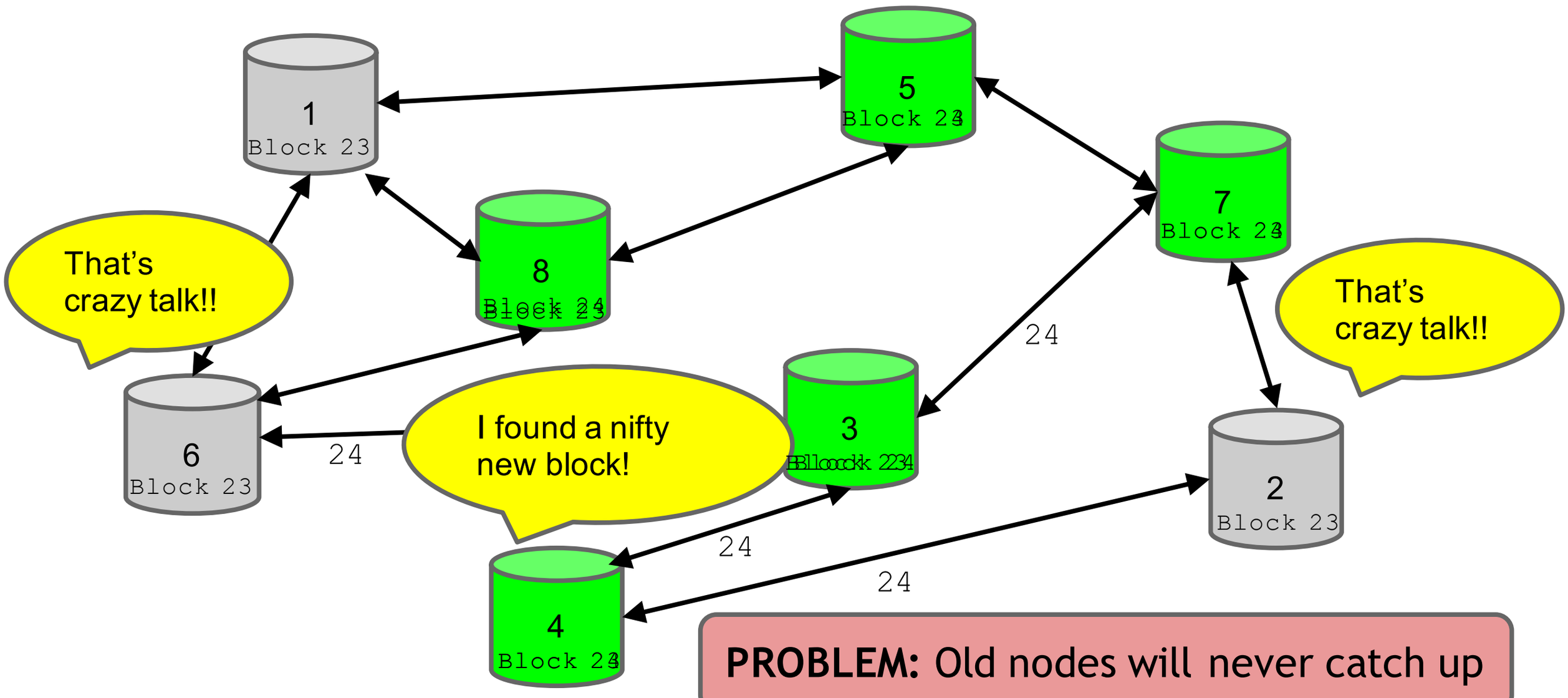


图3.10 区块链的大小

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


1
Block 23
5
Block 24
7
Block 24
8
Block 24
That's crazy talk!!
24
That's crazy talk!!
6
Block 23
24
I found a nifty new block!
3
Block 24
2
Block 23
24
24
4
Block 24
PROBLEM: Old nodes will never catch up

硬 *vs.* 软

比特币存储

Hot storage

online

hot secret key(s)

cold address(es)

payments

Cold storage

offline

威胁

Charles Ponzi

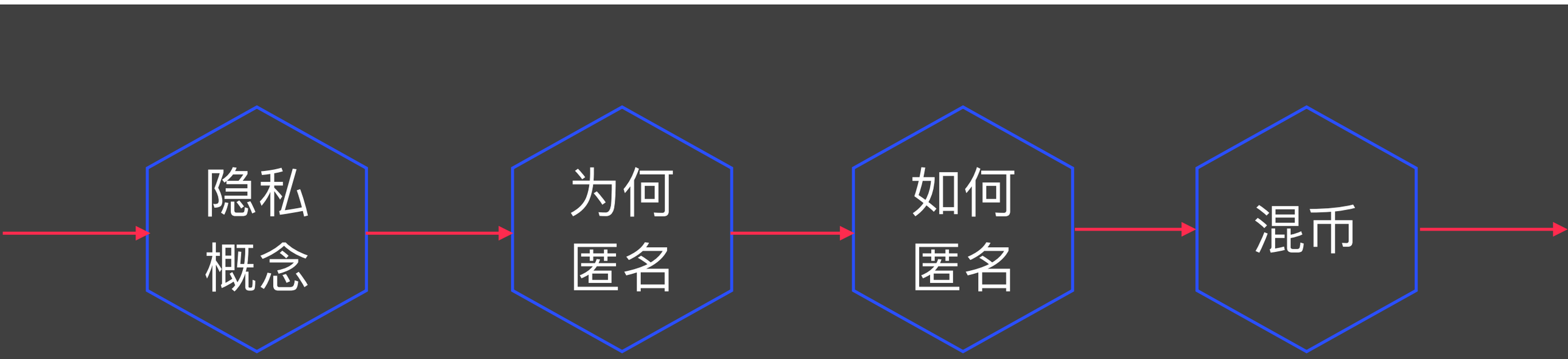
交易所


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
VAIO

比特币限制

- *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



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

隐私：定义

- 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

私人空间

家庭
城邦

公共空间

private：私
privare：剥夺

私人空间

社交空间

公共空间

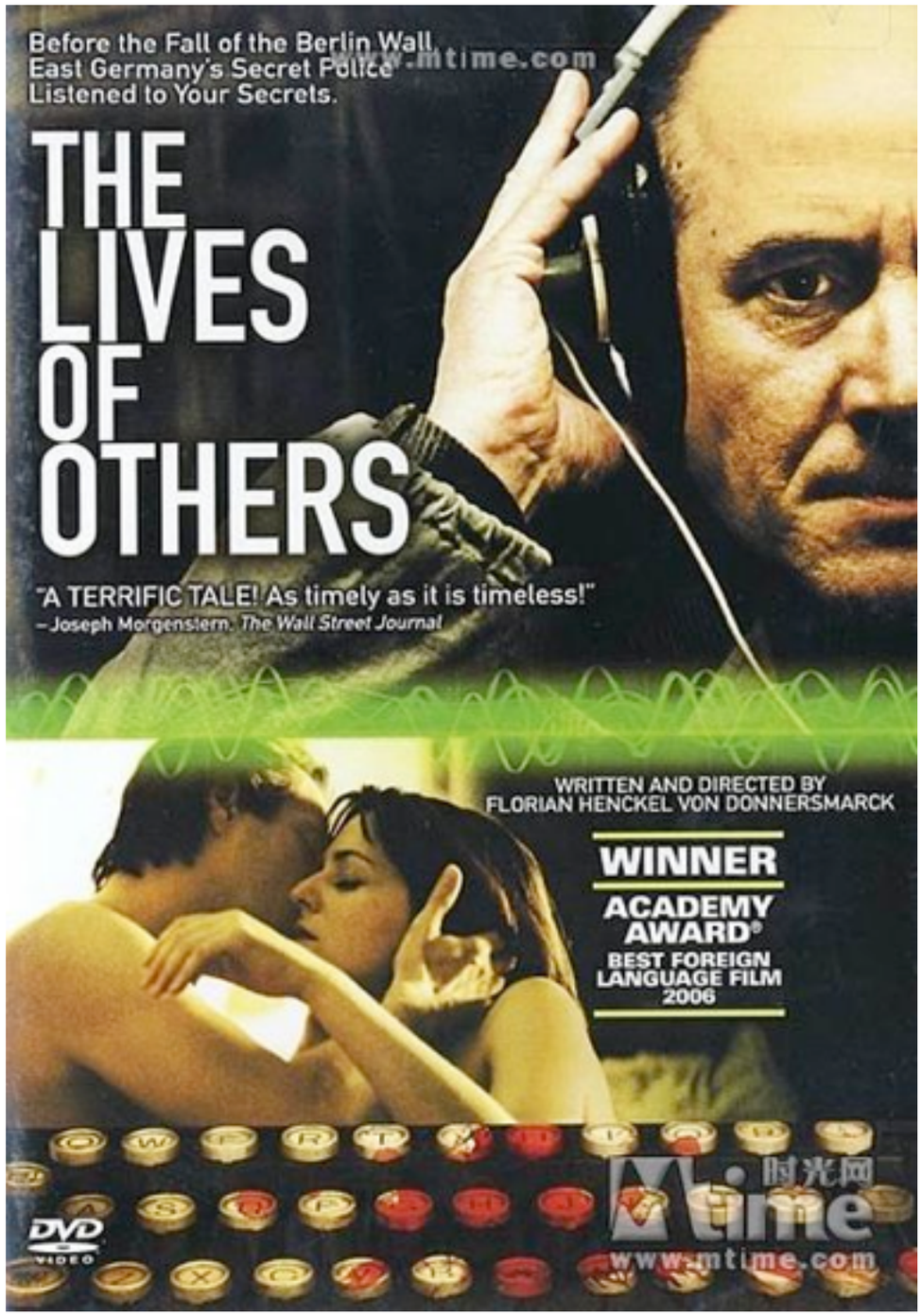
照相机　　摄像机　　网络

摄像头　　闭路监控　　大数据

GPS　　智能手机　　物联网

隐私: 两个电影


1984
The Film of the Year


Before the Fall of the Berlin Wall,
East Germany's Secret Police
Listened to Your Secrets.
THE LIVES OF OTHERS
"A TERRIFIC TALE! As timely as it is timeless!"
– Joseph Morgenstern, The Wall Street Journal
WRITTEN AND DIRECTED BY
FLORIAN HENCKEL VON DONNERSMARCK
WINNER
ACADEMY AWARD®
BEST FOREIGN LANGUAGE FILM
2006
DVD
www.mtime.com

隐私：相关事件

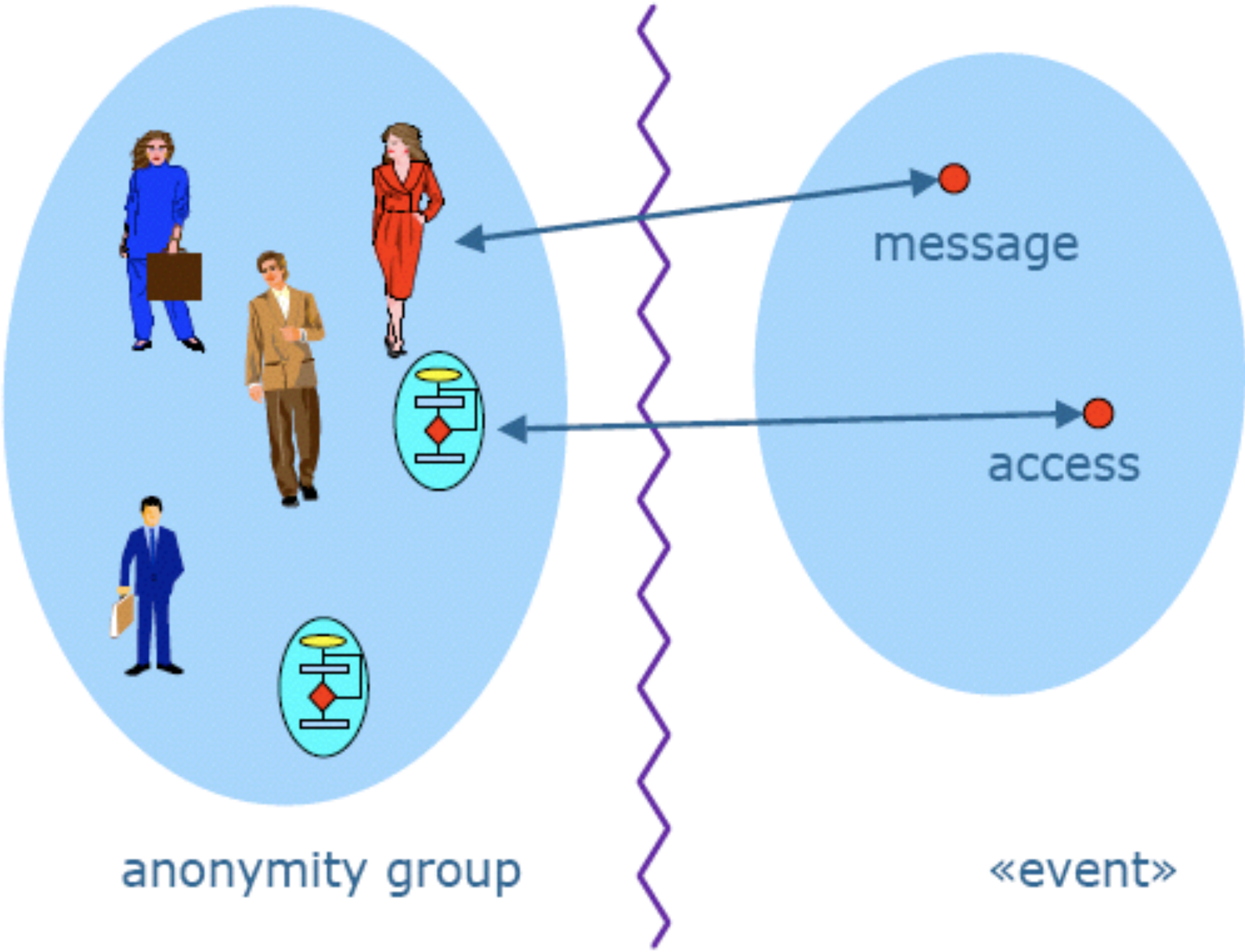
http://maherarar.net/

Cambridge Analytica

facebook

Google:
Don't be evil.

隐私保护



无关联性

比特币的匿名性

- 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

比特币为什么需要匿名

- 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

K匿名

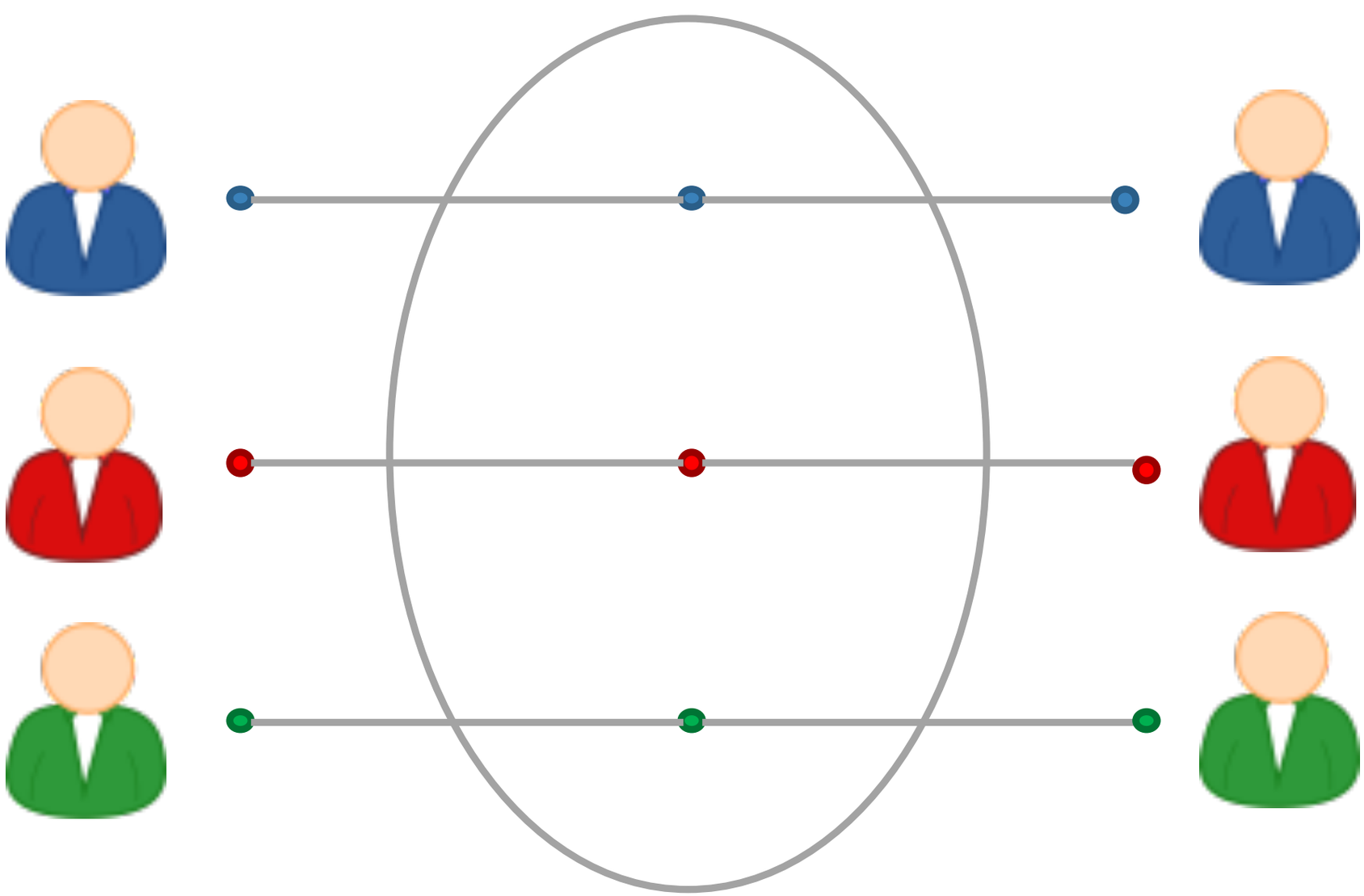
Name	Age	Gender	State of domicile	Religion	Disease
Ramsha	29	Female	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	Kerala	Hindu	Viral infection
Salima	28	Female	Tamil Nadu	Muslim	TB
sunny	27	Male	Karnataka	Parsi	No illness
Joan	24	Female	Kerala	Christian	Heart-related
Bahuksana	23	Male			
Rambha	19	Male			
Kishor	29	Male			
Johnson	17	Male			
John	19	Male			

数据脱敏

匿名集合

Name	Age	Gender	State of domicile	Religion	Disease
*	20 < Age ≤ 30	Female	Tamil Nadu	*	Cancer
*	20 < Age ≤ 30	Female	Kerala	*	Viral infection
*	20 < Age ≤ 30	Female	Tamil Nadu	*	TB
*	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

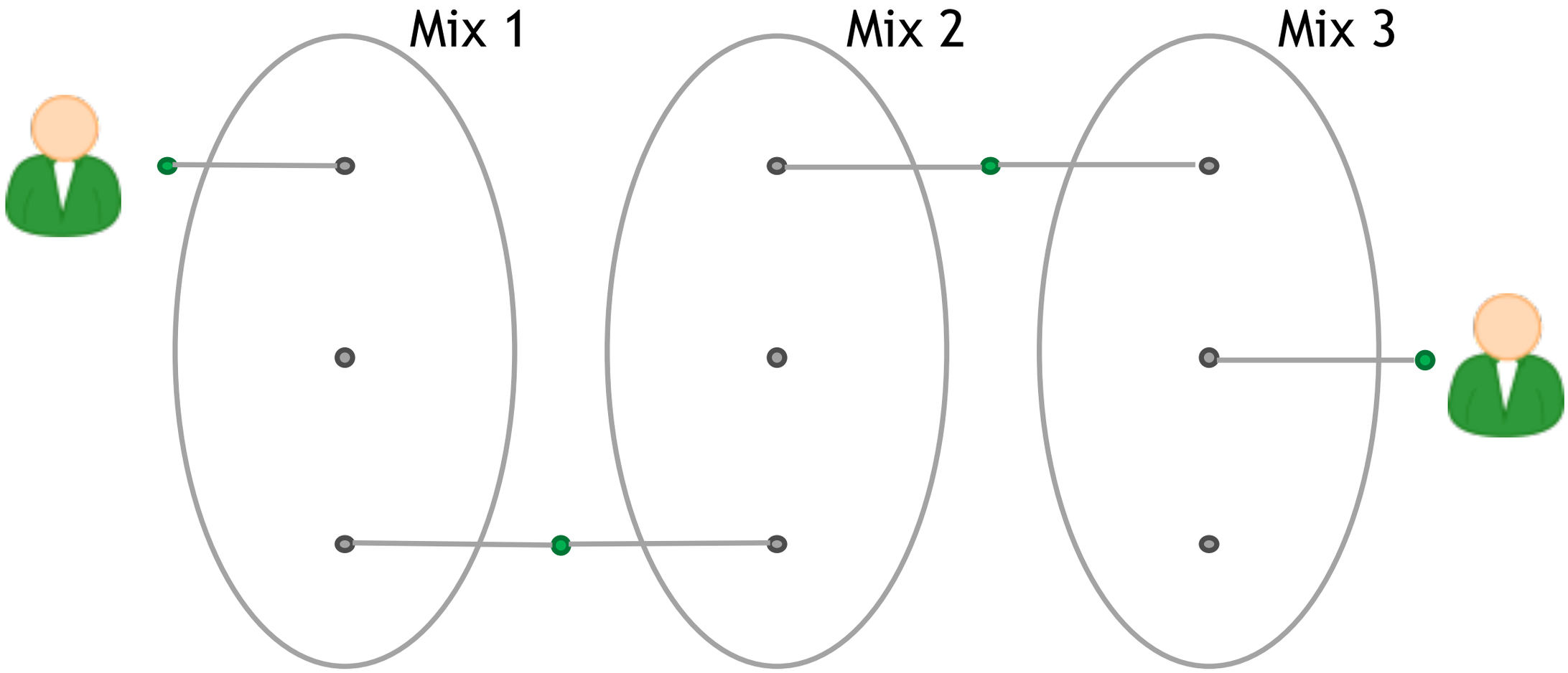


在线钱包

引入中介节点

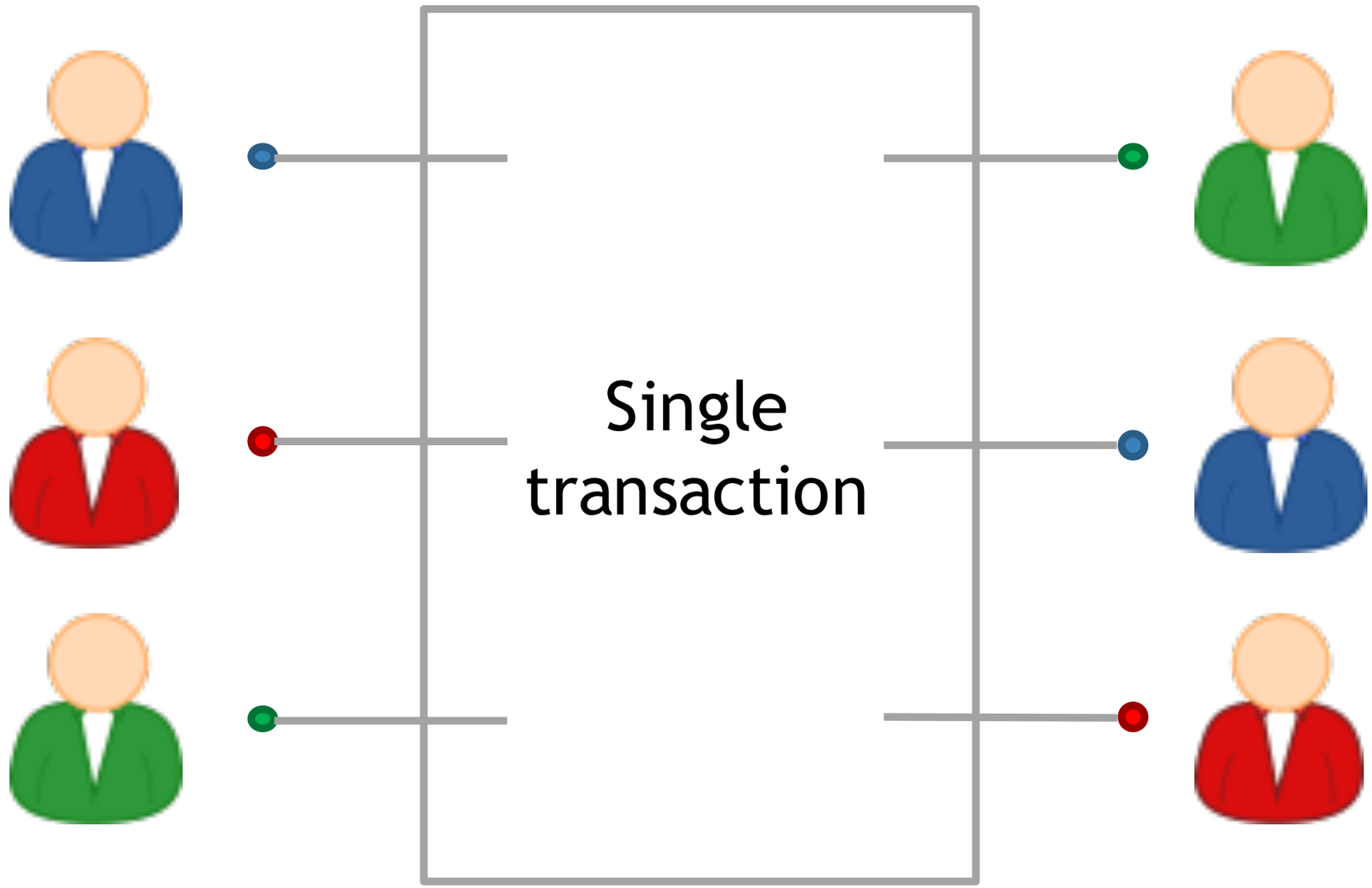
专项服务

多层混币



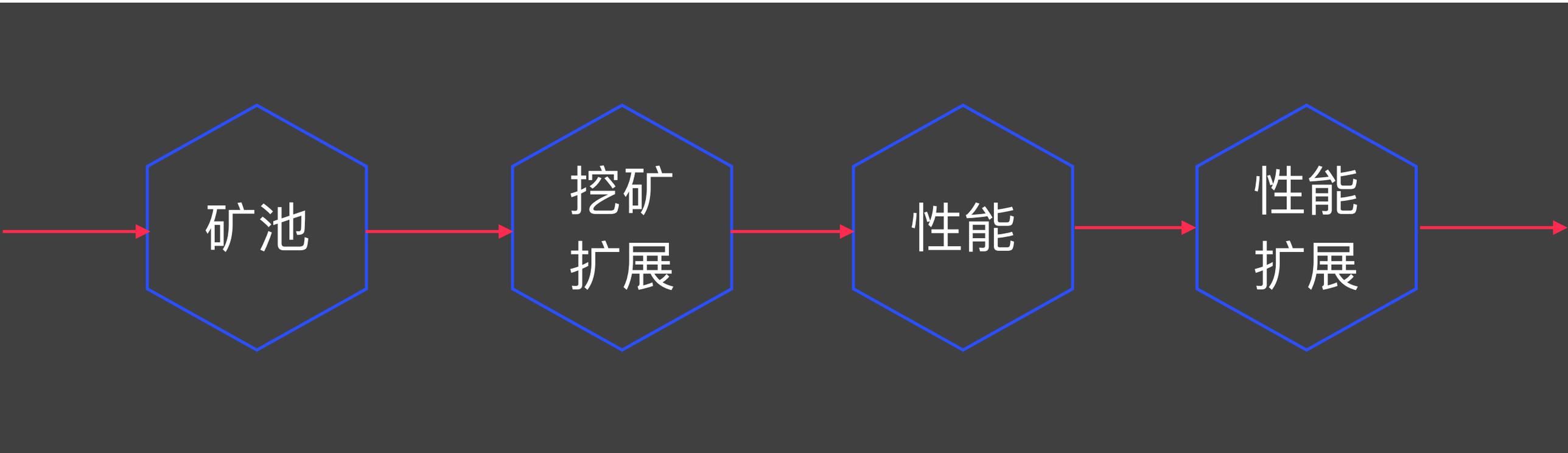
多重

分布式混币



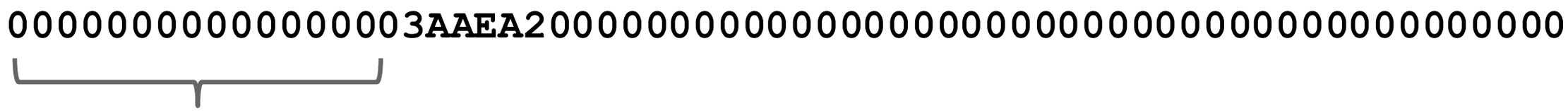
分布式

扩展



挖矿难度

256 bit hash output



当前难度 $= 2^{66.2}$

$$\text{下一个难度} = \frac{\text{上一个难度} * 2016 * 10\text{分钟}}{\text{产生上2016个区块所花费时间}}$$

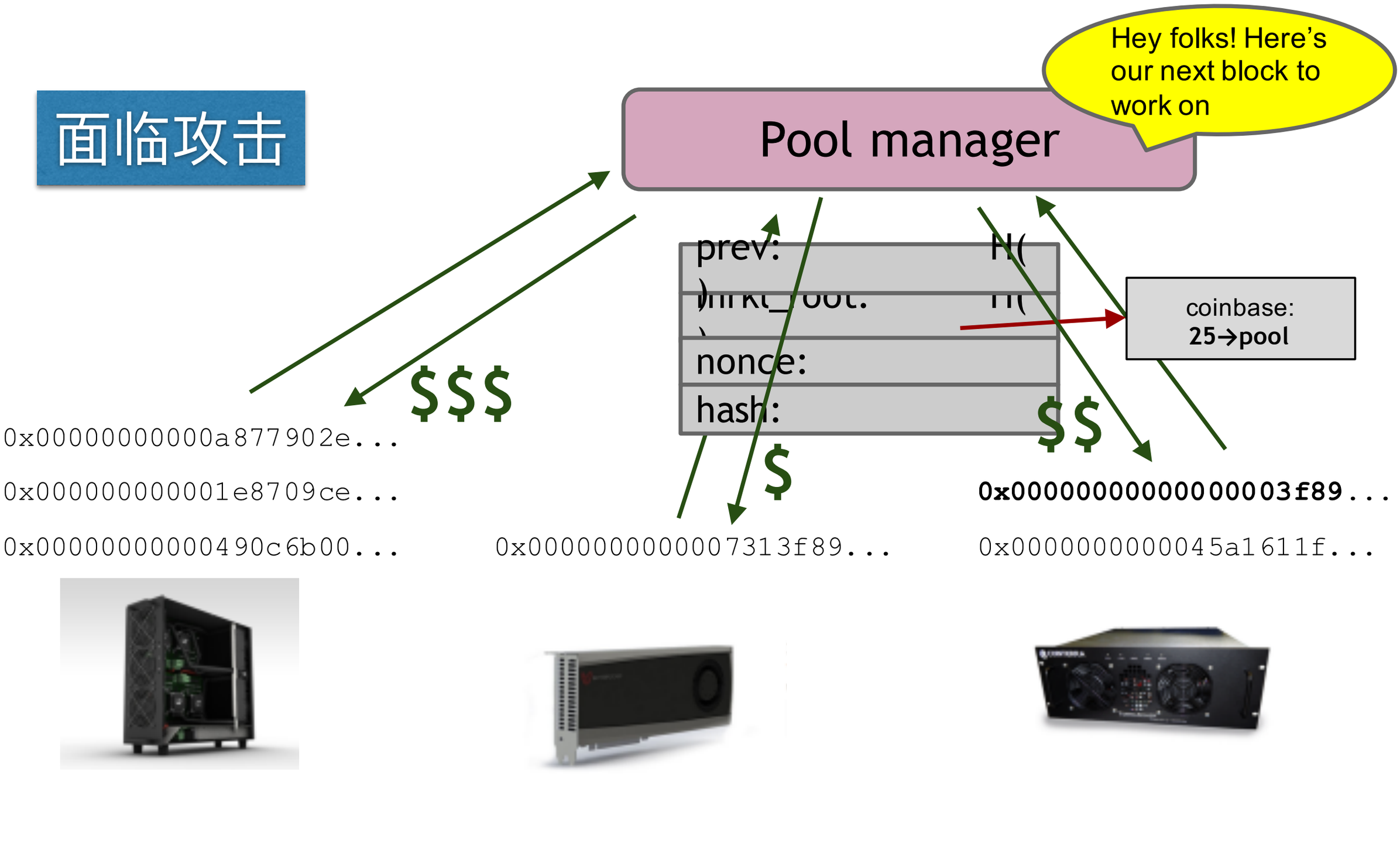
挖矿互助

输出接近结果的挖矿结果来证明自己的工作量

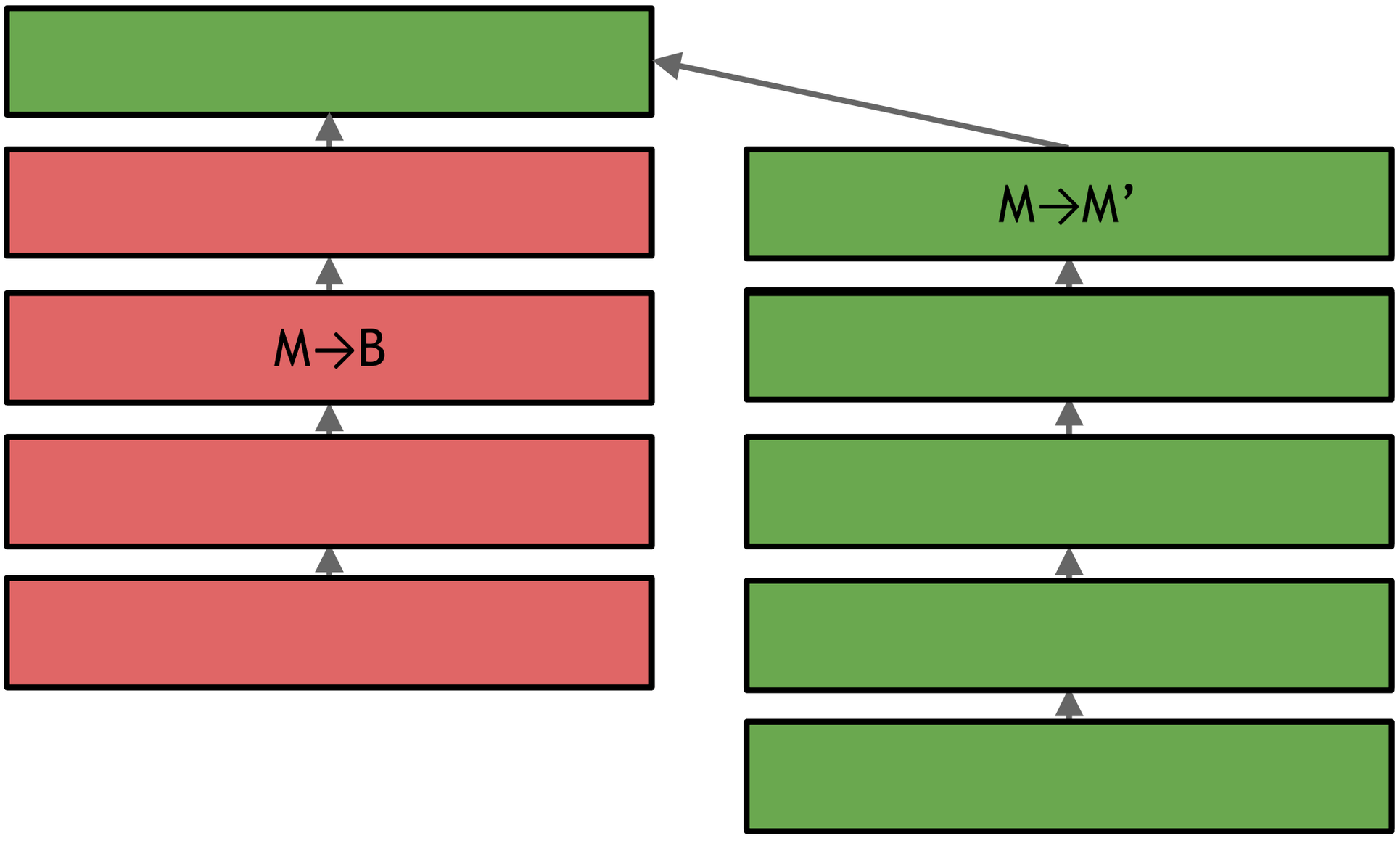
```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
009048813379E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
00000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E7761384561 81FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
00000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

矿池模式

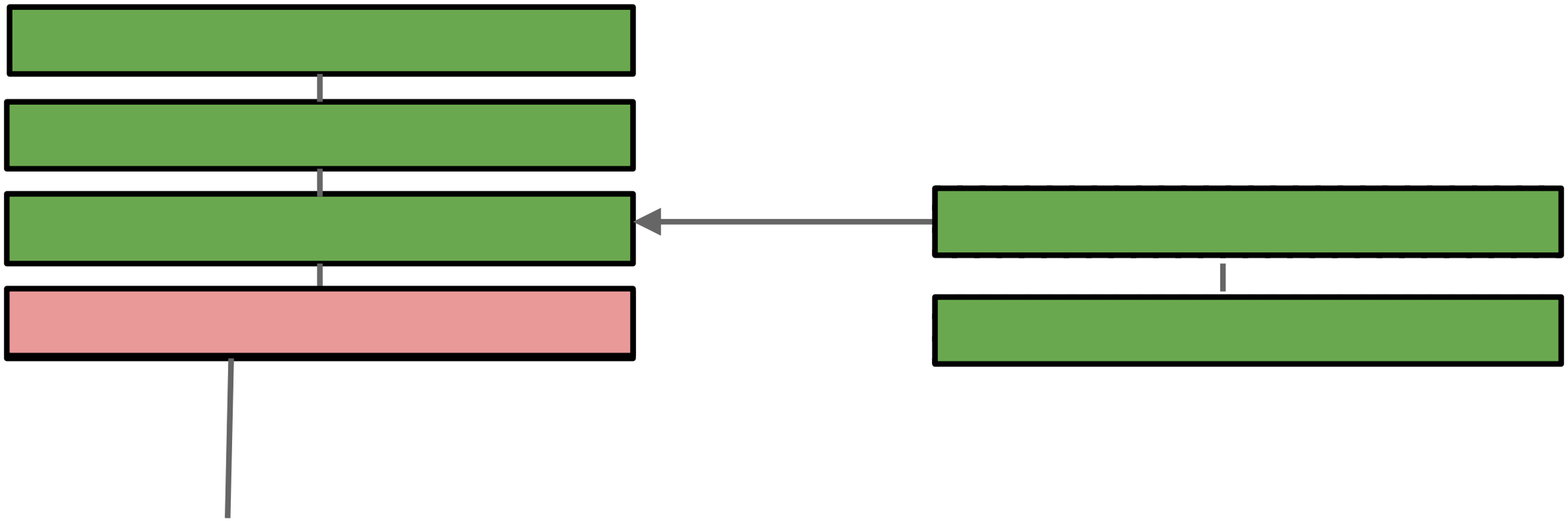
面临攻击


Hey folks! Here's our next block to work on
Pool manager
prev:
H(
)
mrkl_root:
H(
)
nonce:
hash:
coinbase:
25→pool
$$$
$
$$
0x00000000000a877902e...
0x000000000001e8709ce...
0x0000000000490c6b00...
0x0000000000007313f89...
0x0000000000000003f89...
0x0000000000045a1611f...

分叉攻击



临时保留区块攻击



All other miners are wasting effort here!

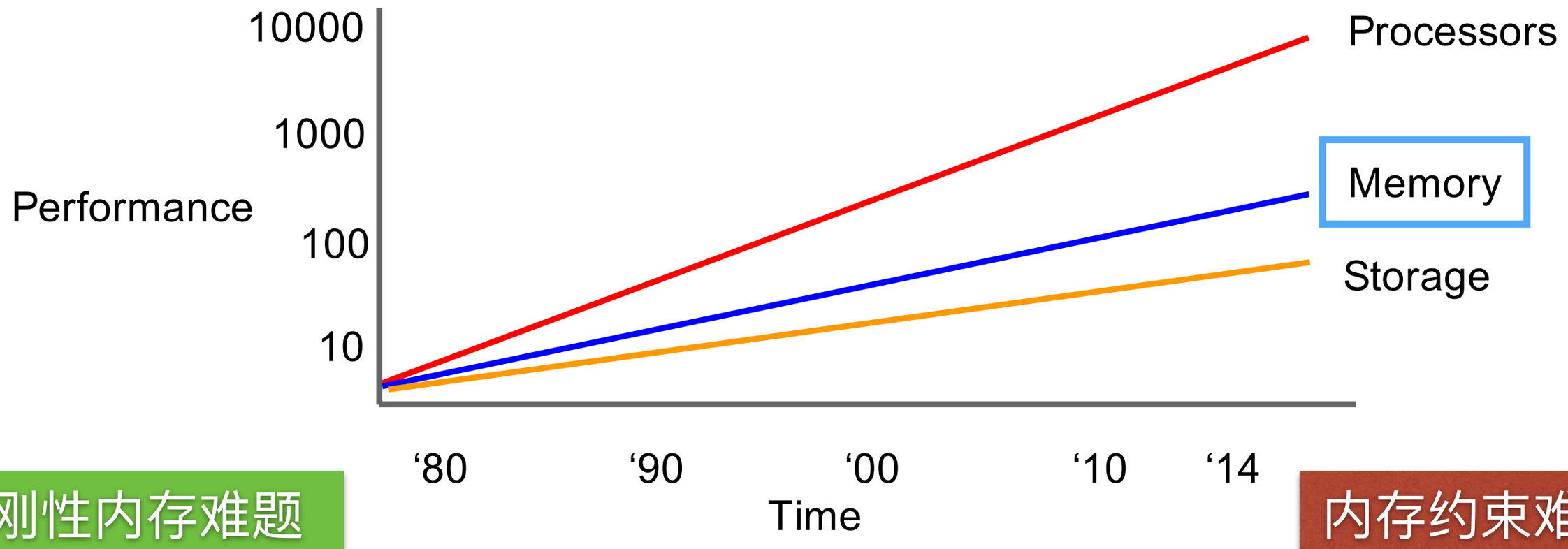
挖矿算法基本要求

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

反ASIC



刚性内存难题

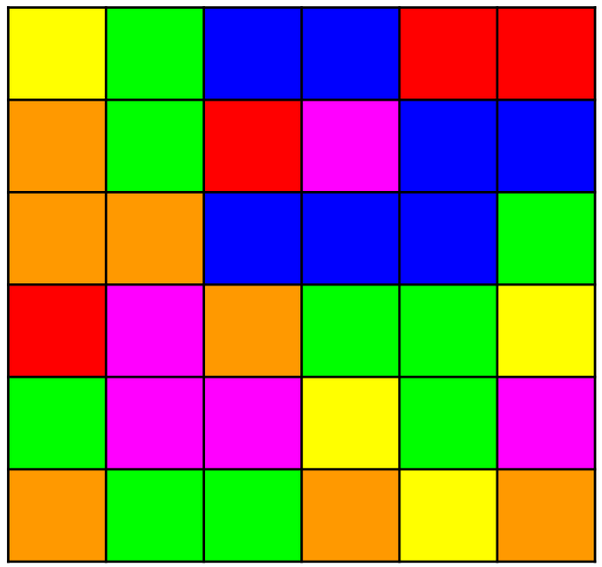
内存约束难题

Scrypt

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

XI I

参数

反ASIC是否可能

SHA256

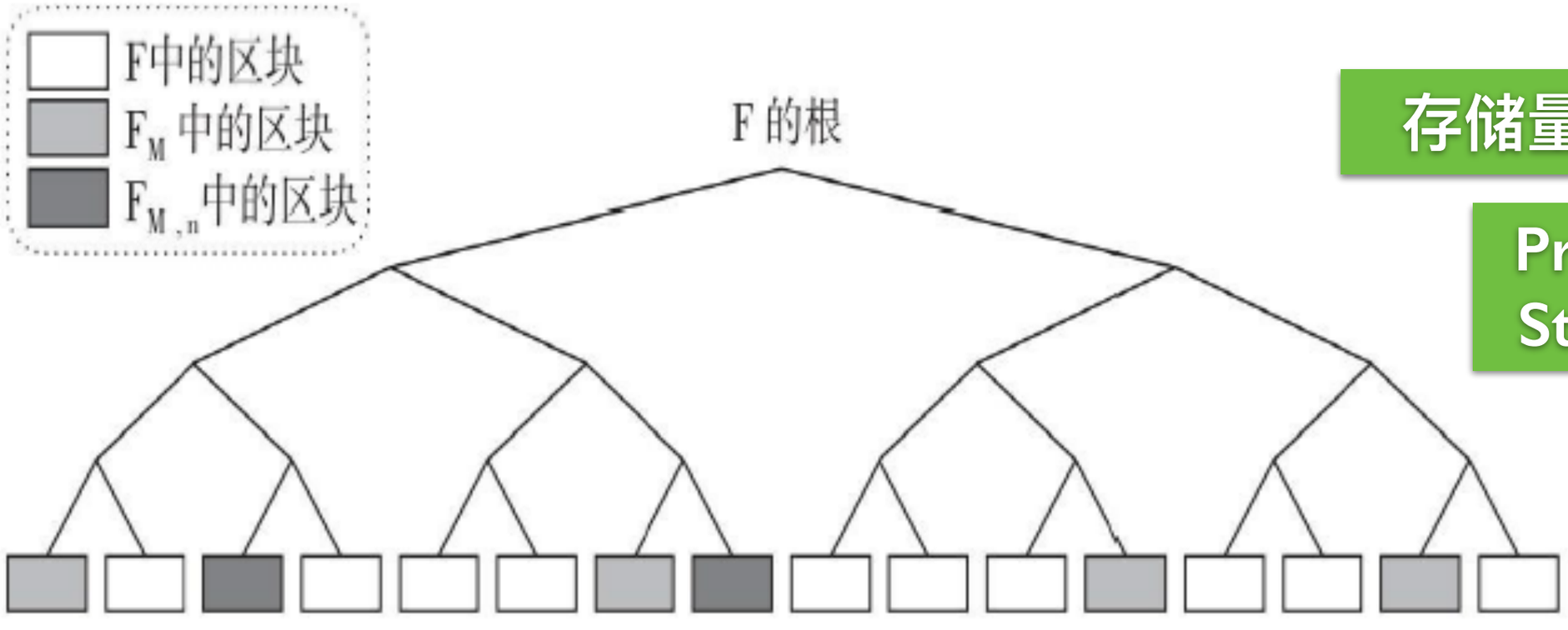
反ASIC是否有问题

有效工作量证明

挖矿能量消耗问题

志愿者计算项目

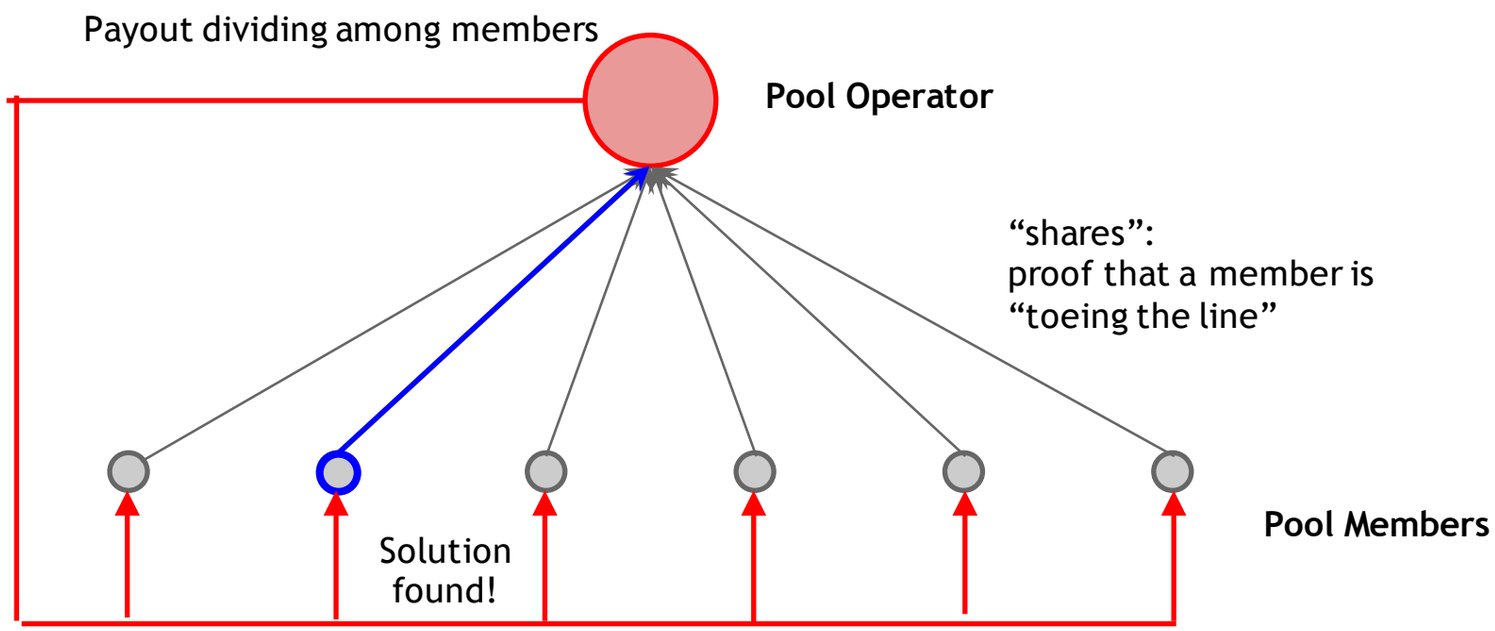
分布式存储



存储量证明

Proof of Storage

不可外包的难题



防止矿池的产生

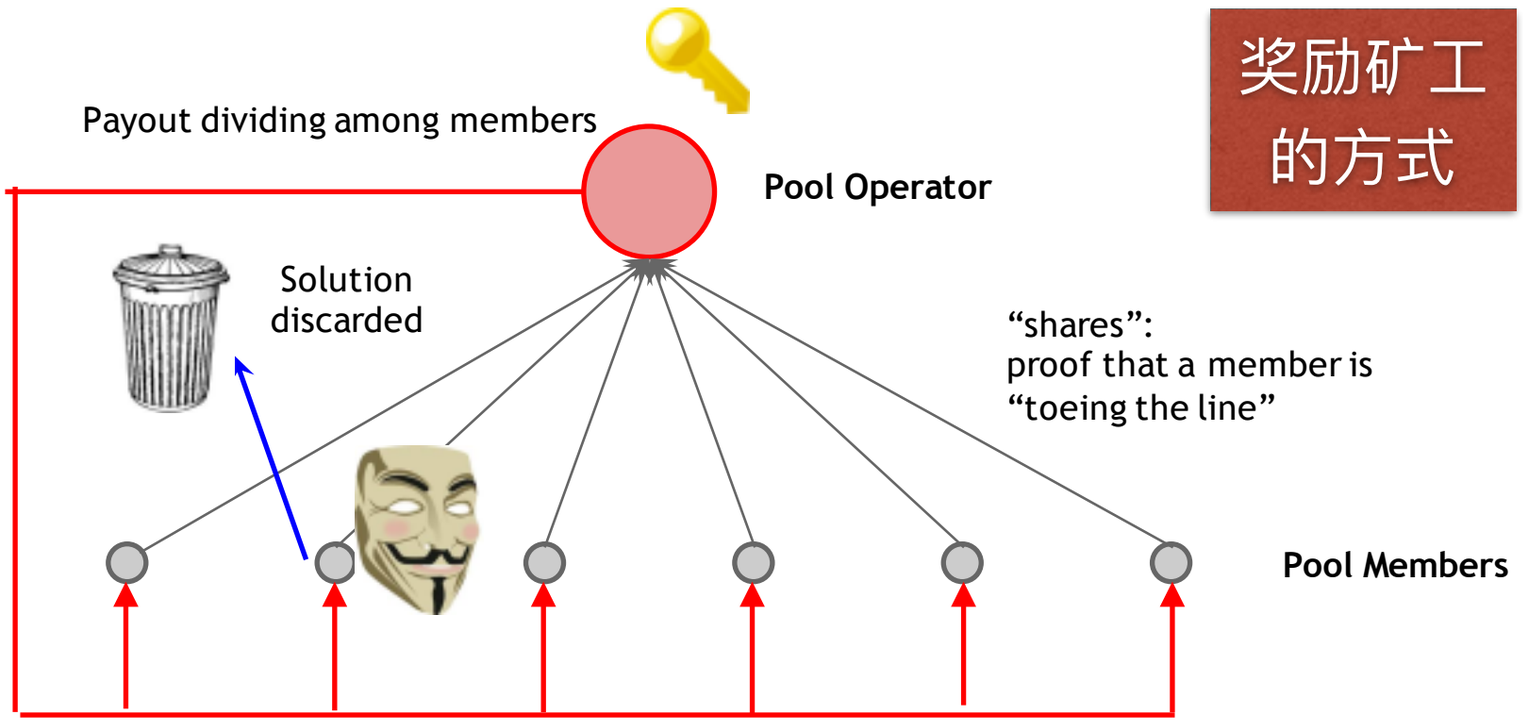
中心化、安全

区块丢弃攻击

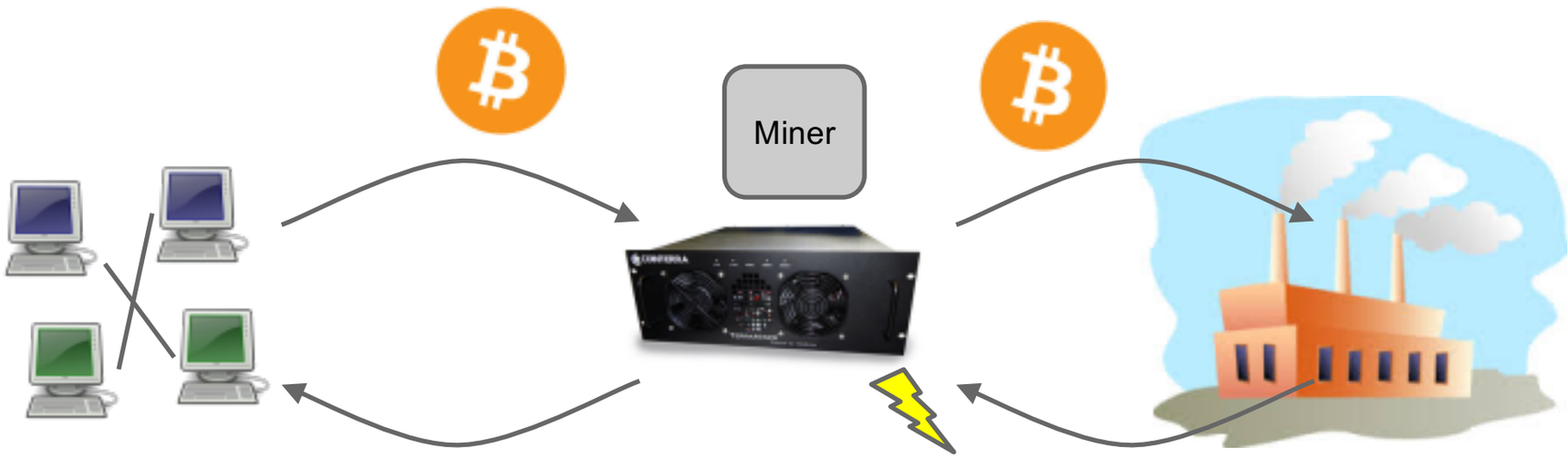
奖励破坏

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



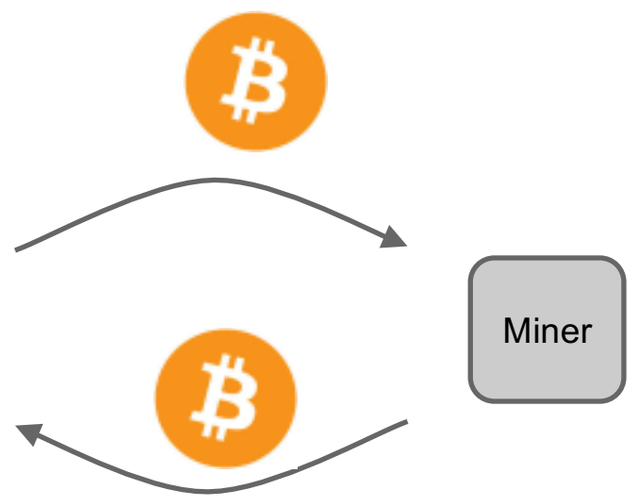
虚拟挖矿



权益证明

分叉攻击

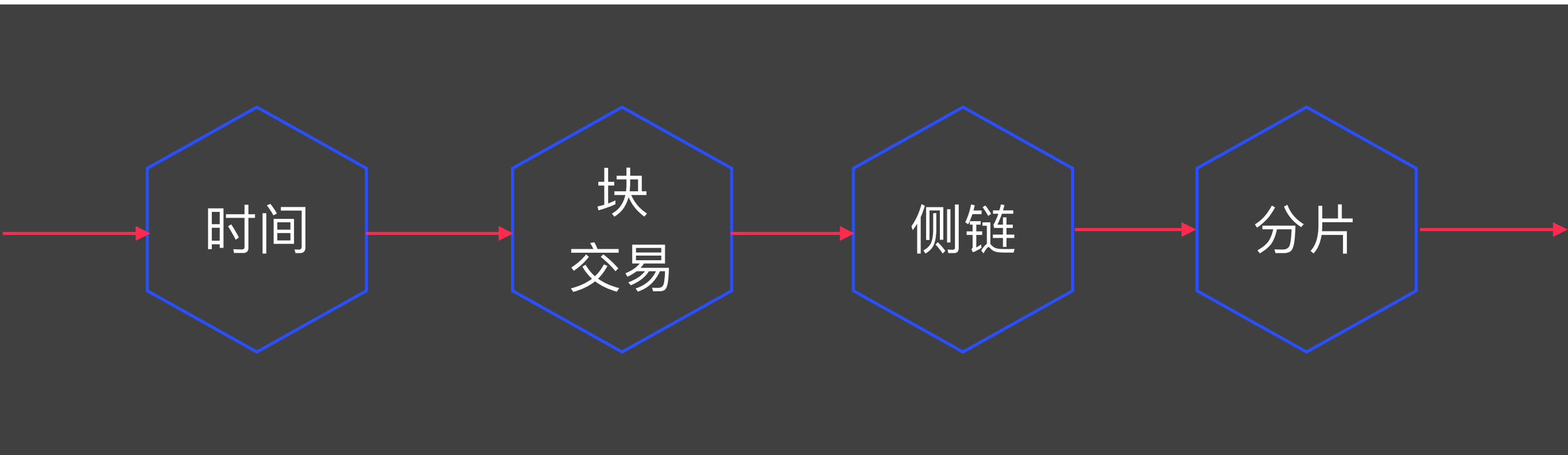
检查点



2012 点点币

币拥有量交易

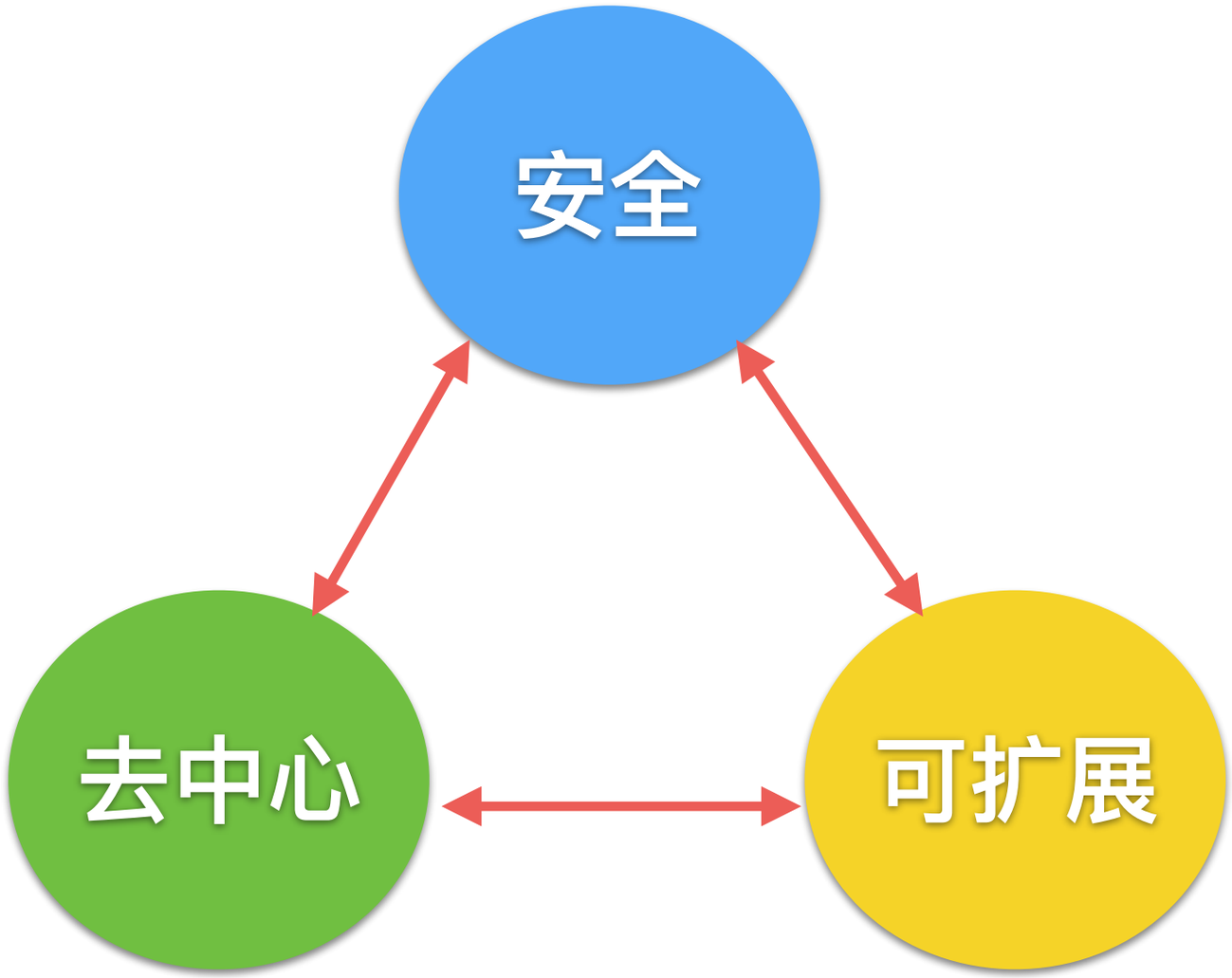
可扩展性



区块链可扩展性

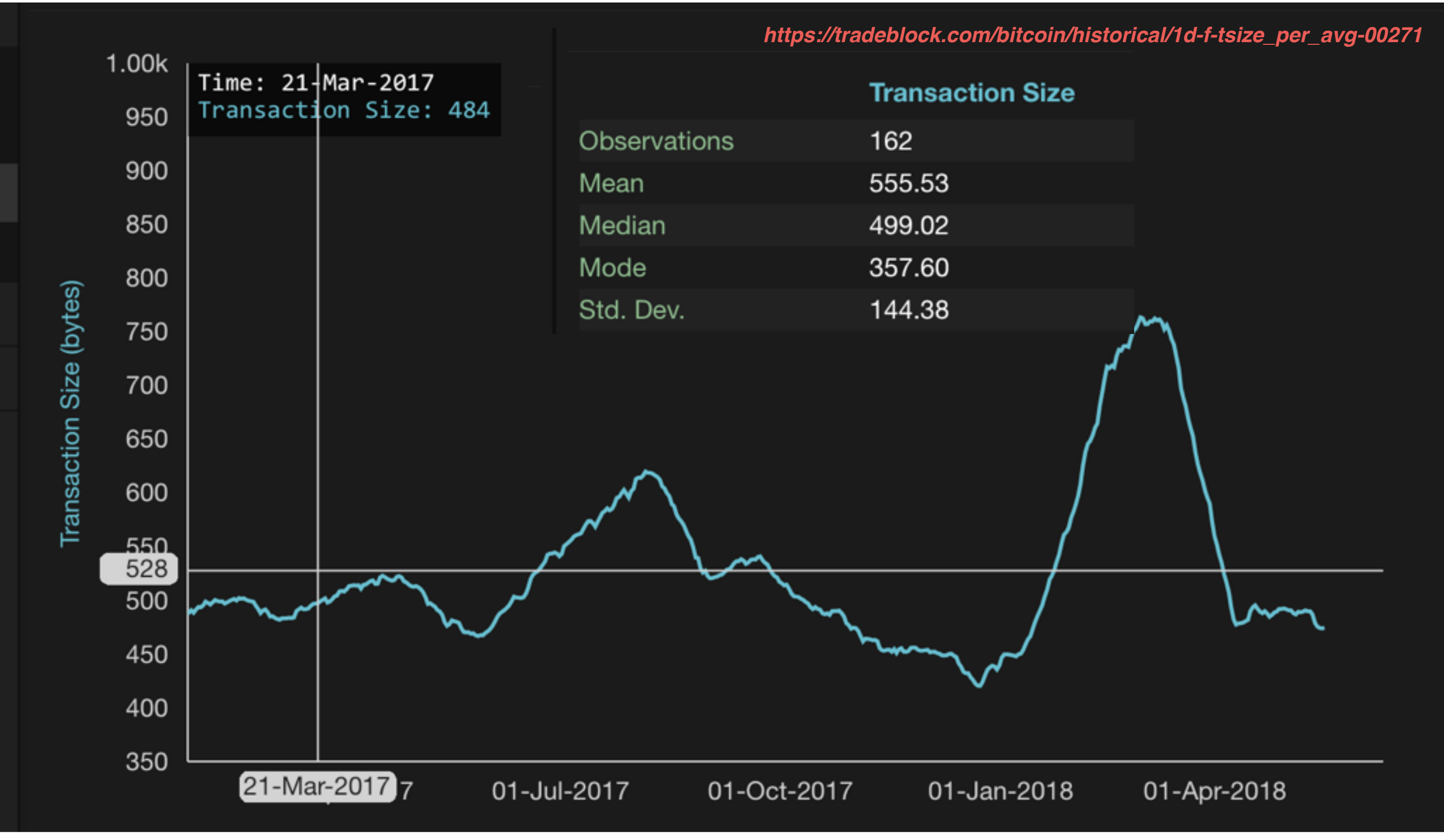
交易容量

产生块时间



比特币的TPS

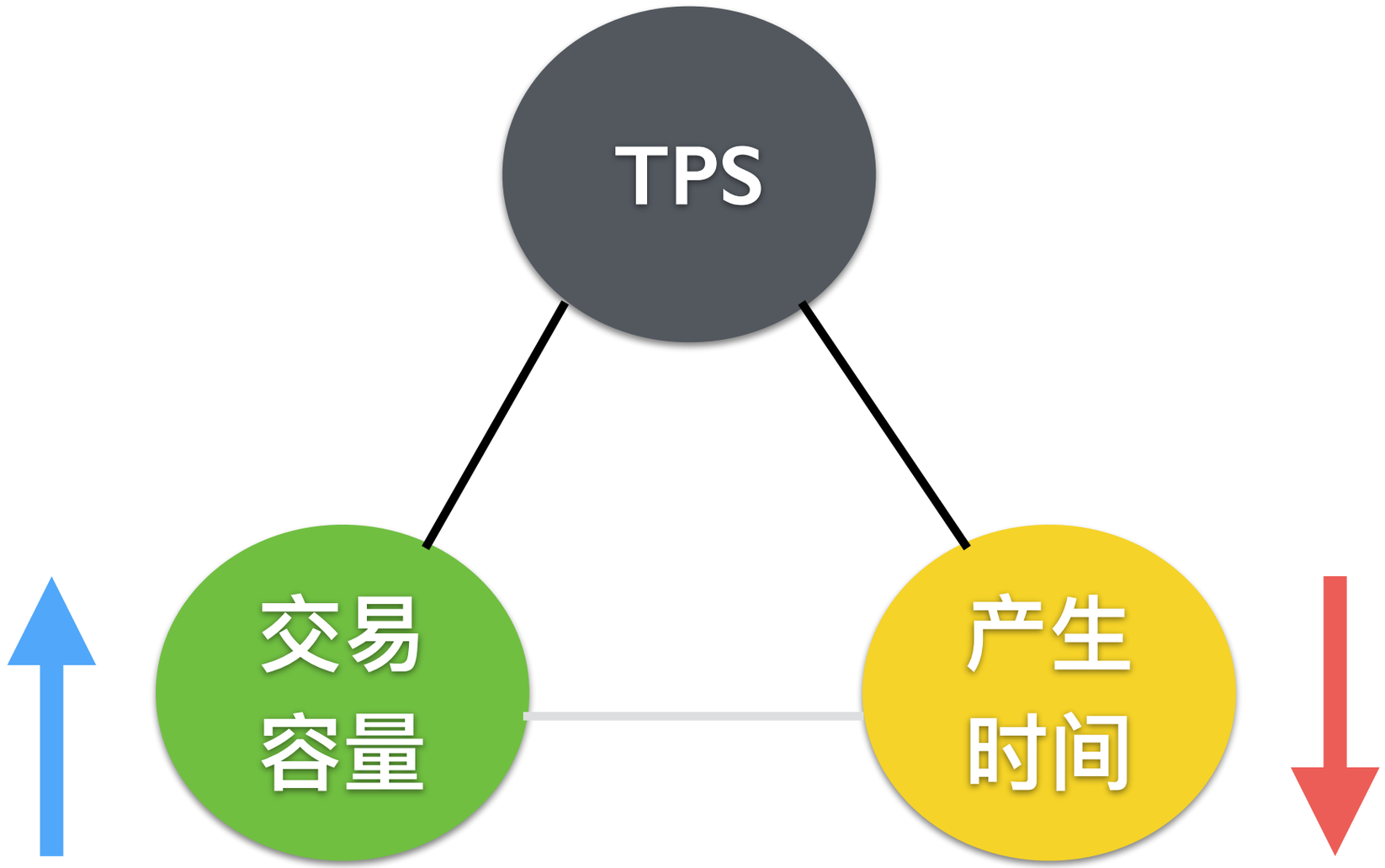
https://tradeblock.com/bitcoin/historical/1d-f-tsize_per_avg-00271



没有比较没有伤害

	3	3.2
PayPal™	150	450
VISA	2000	56000

可扩展性



交易大小　　块的大小

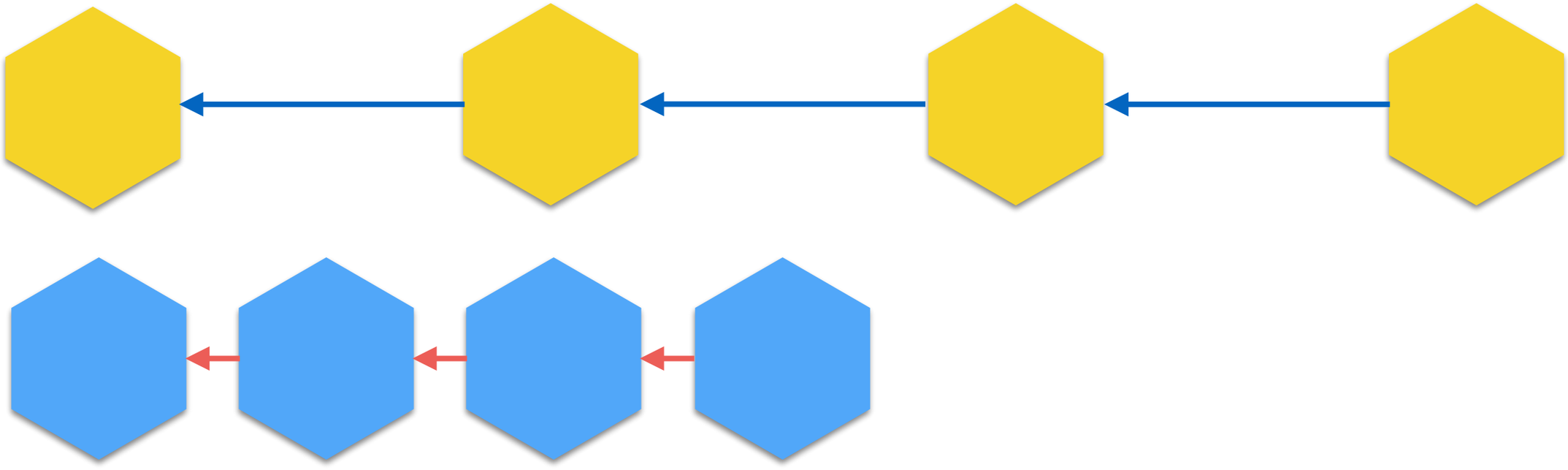
减少块产生时间

块传播时间

块产生时间

块传播时间

块产生时间



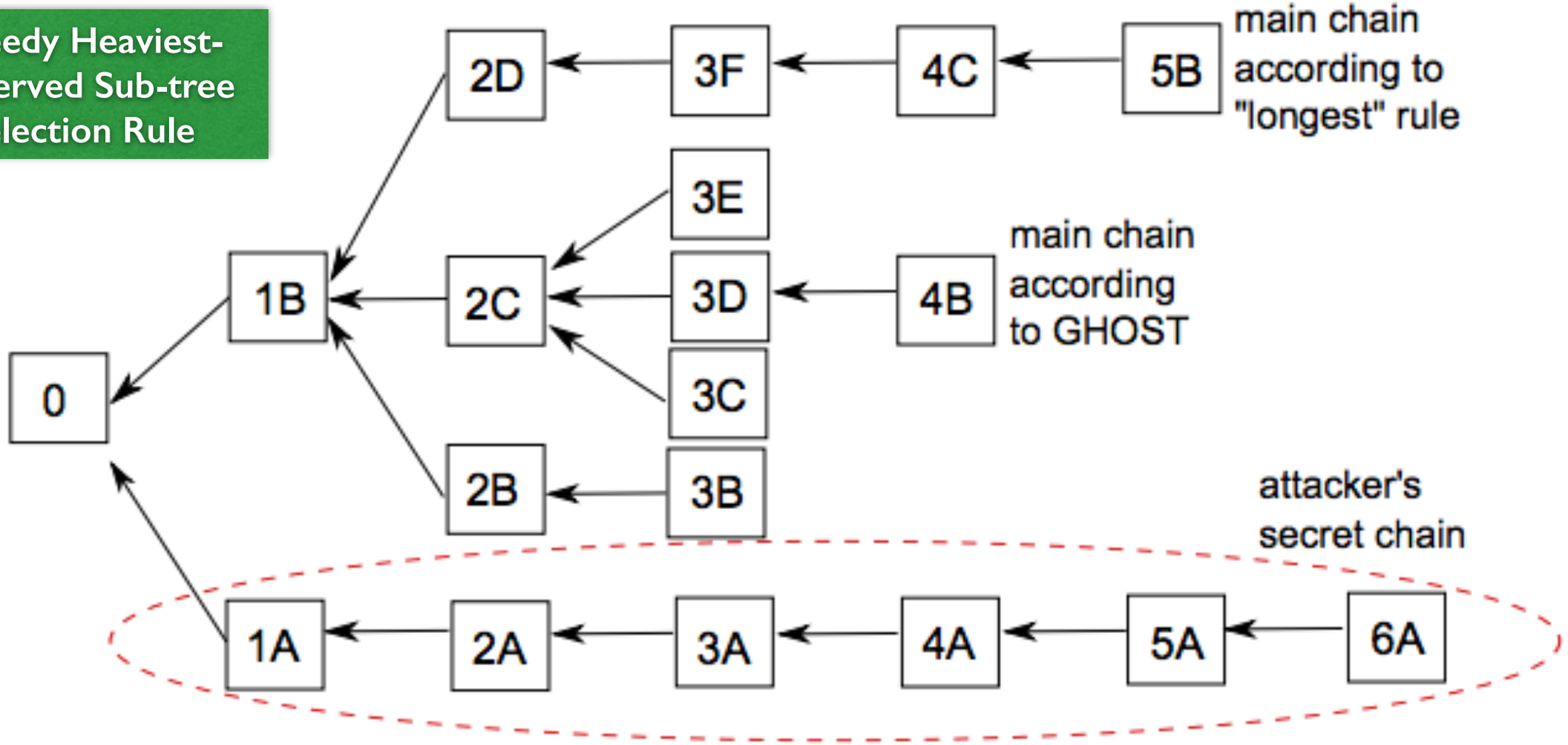
GHOST协议

http://www.avivz.net/pubs/15/btc_ghost_full.pdf

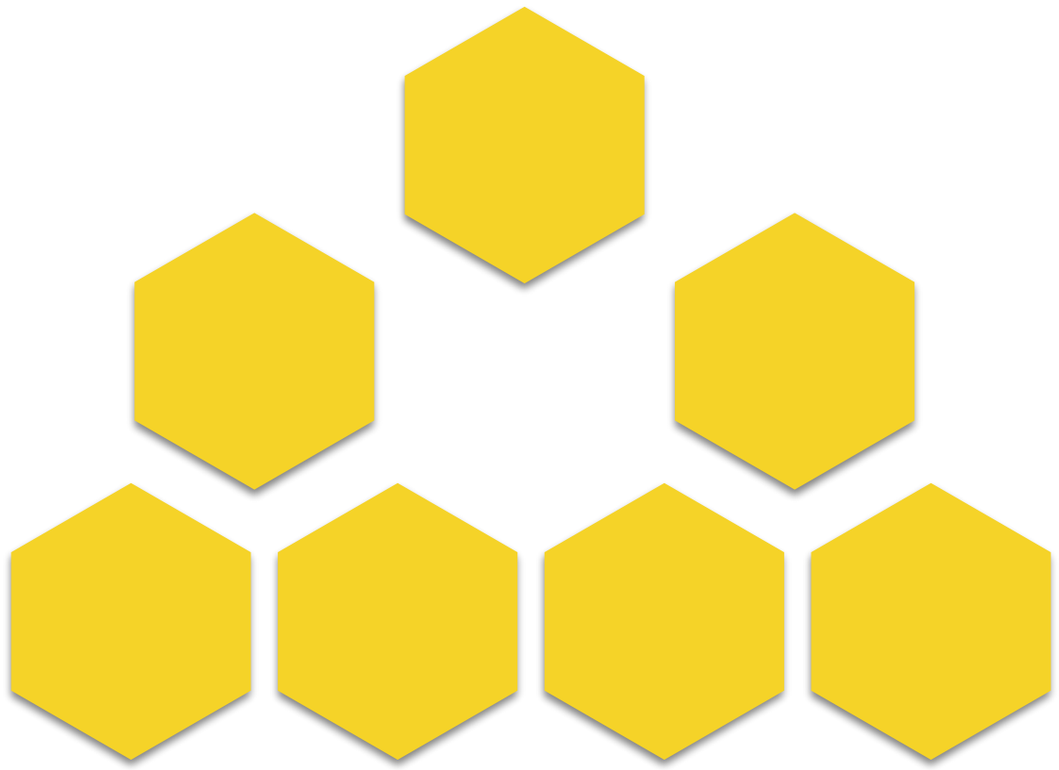
Secure High-Rate Transaction Processing in Bitcoin

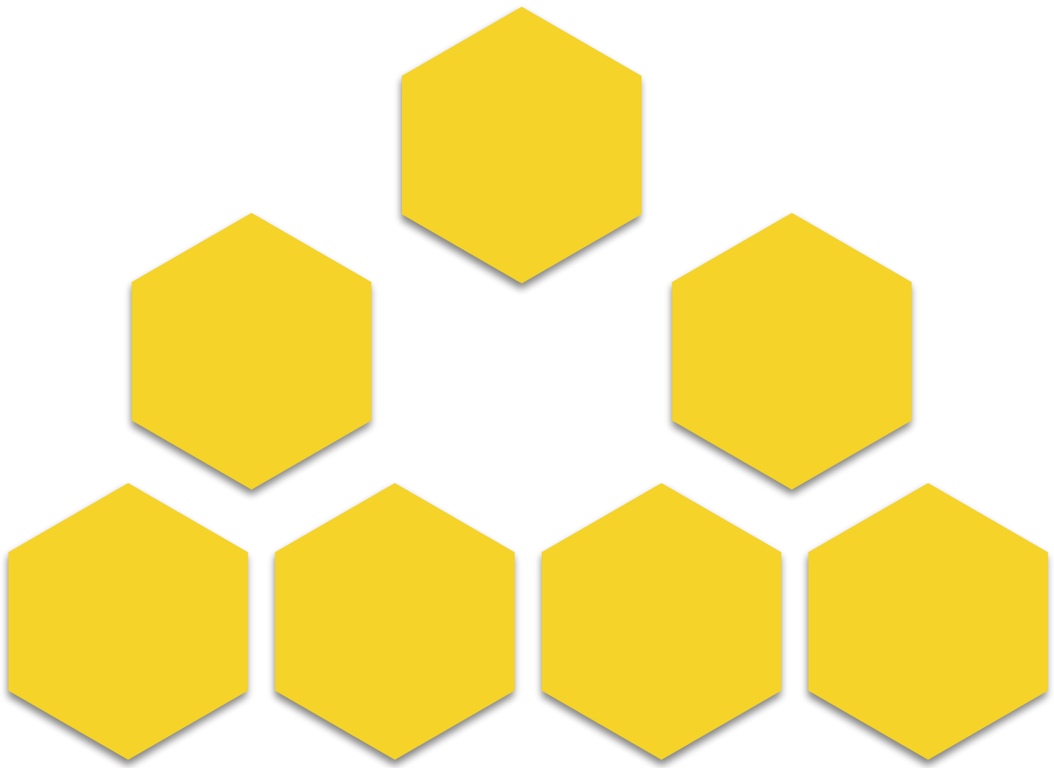
Financial Cryptography and Data Security 2015

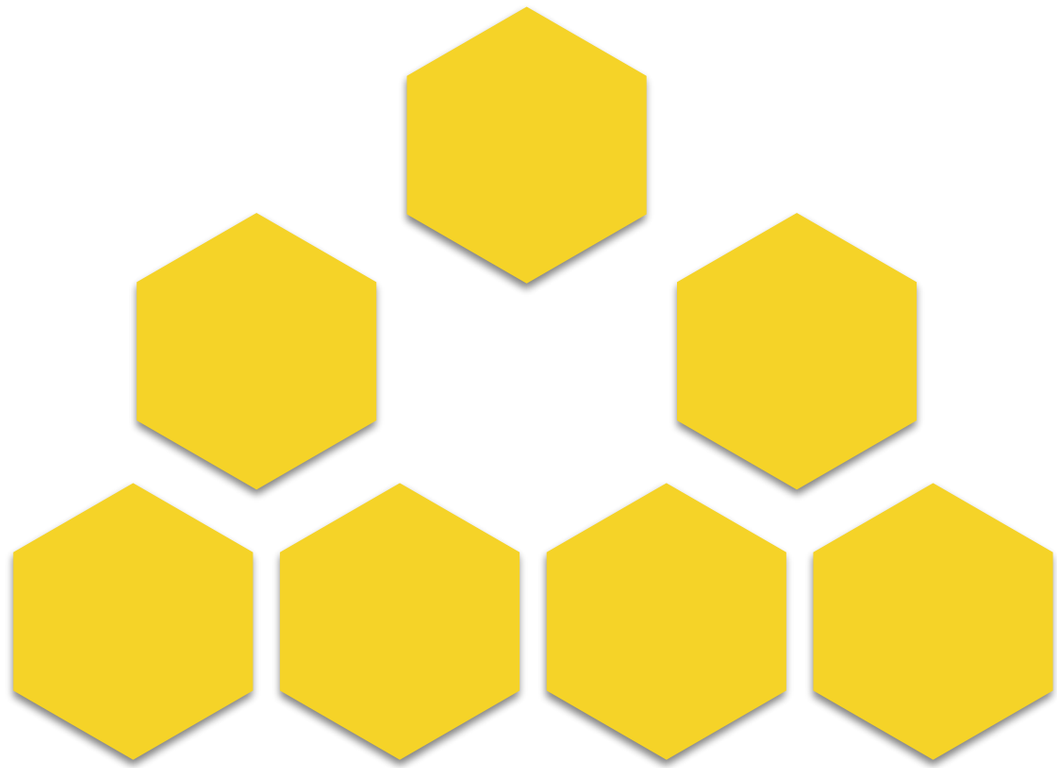
Greedy Heaviest-Observed Sub-tree selection Rule



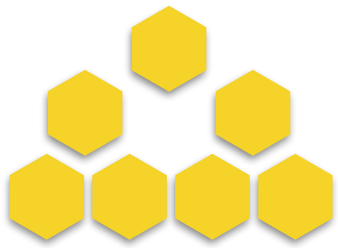
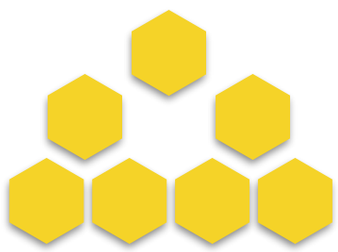
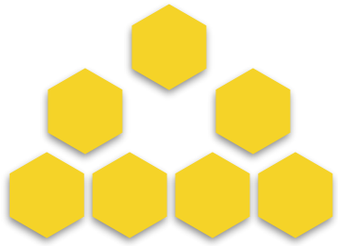
增大块大小







增大块大小

容易执行

更低的成本

矿工同意即可

硬分叉

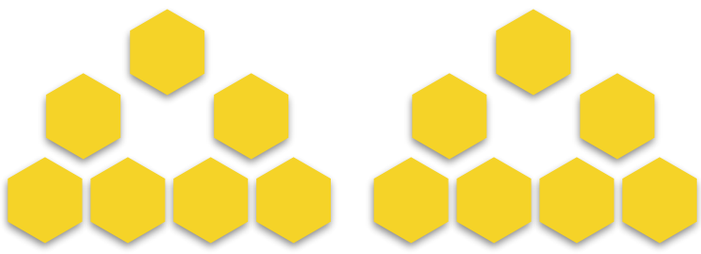
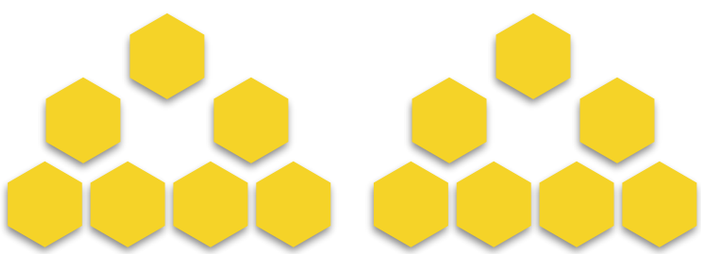
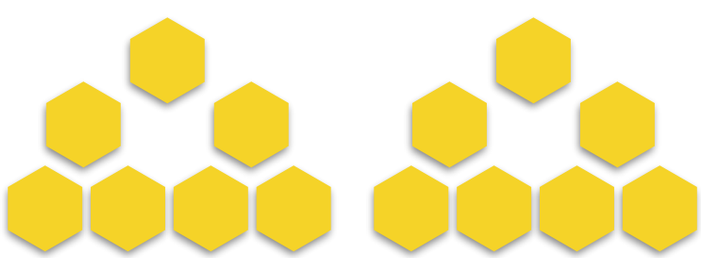
计算能力

更长的传播时间

大小增长块

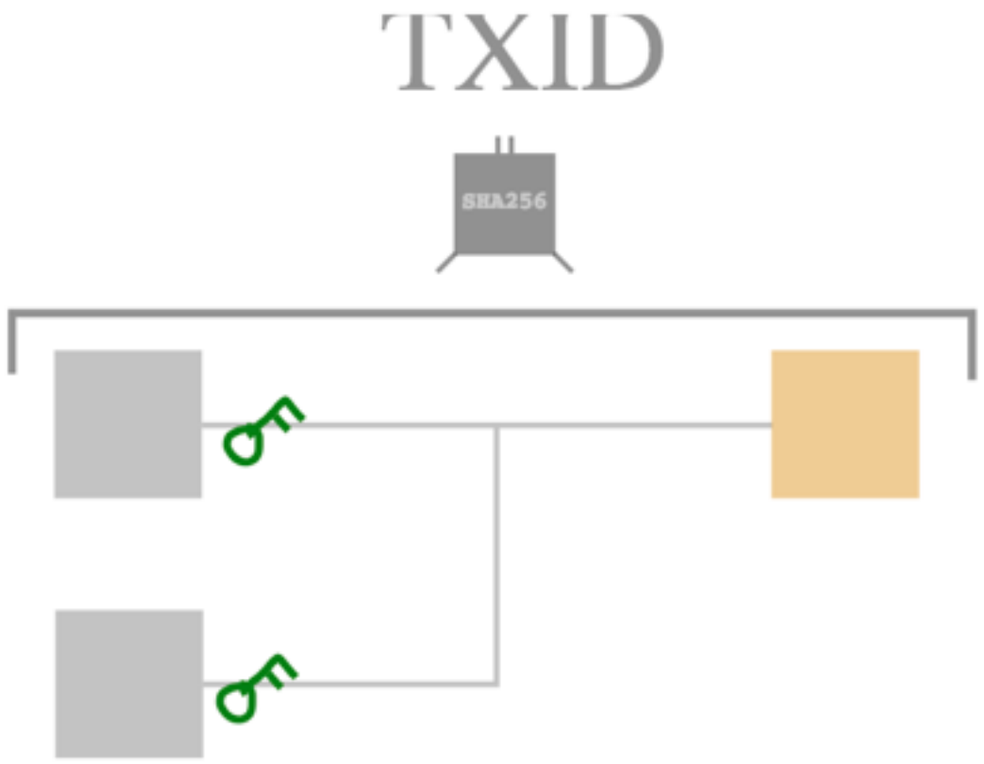
挖矿设备

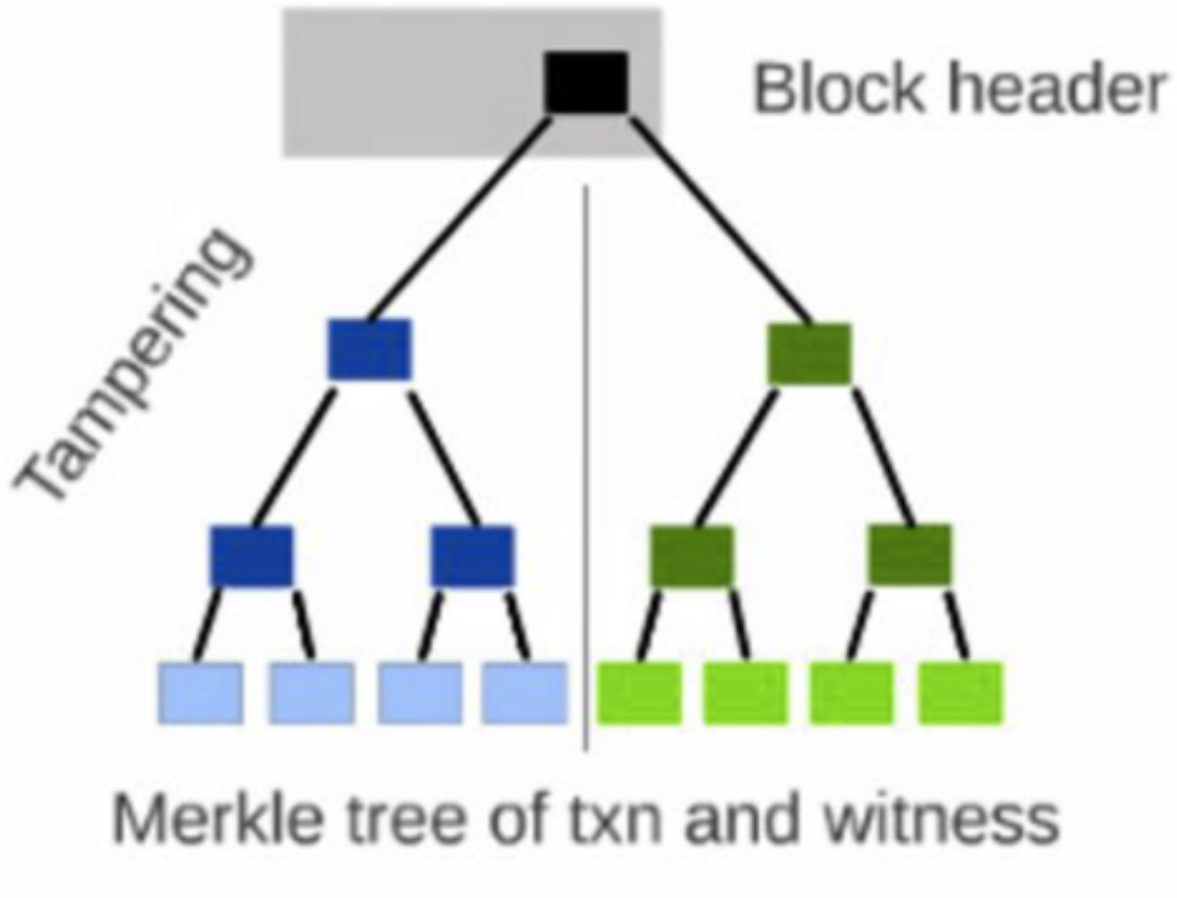
安全性

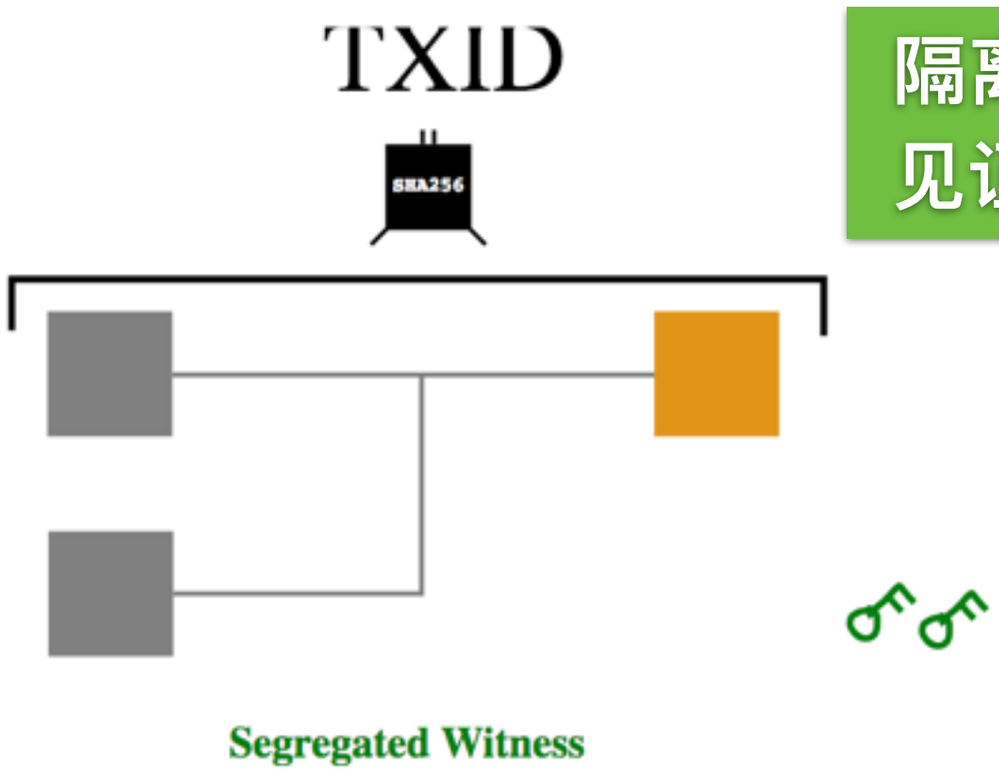




减少交易大小

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





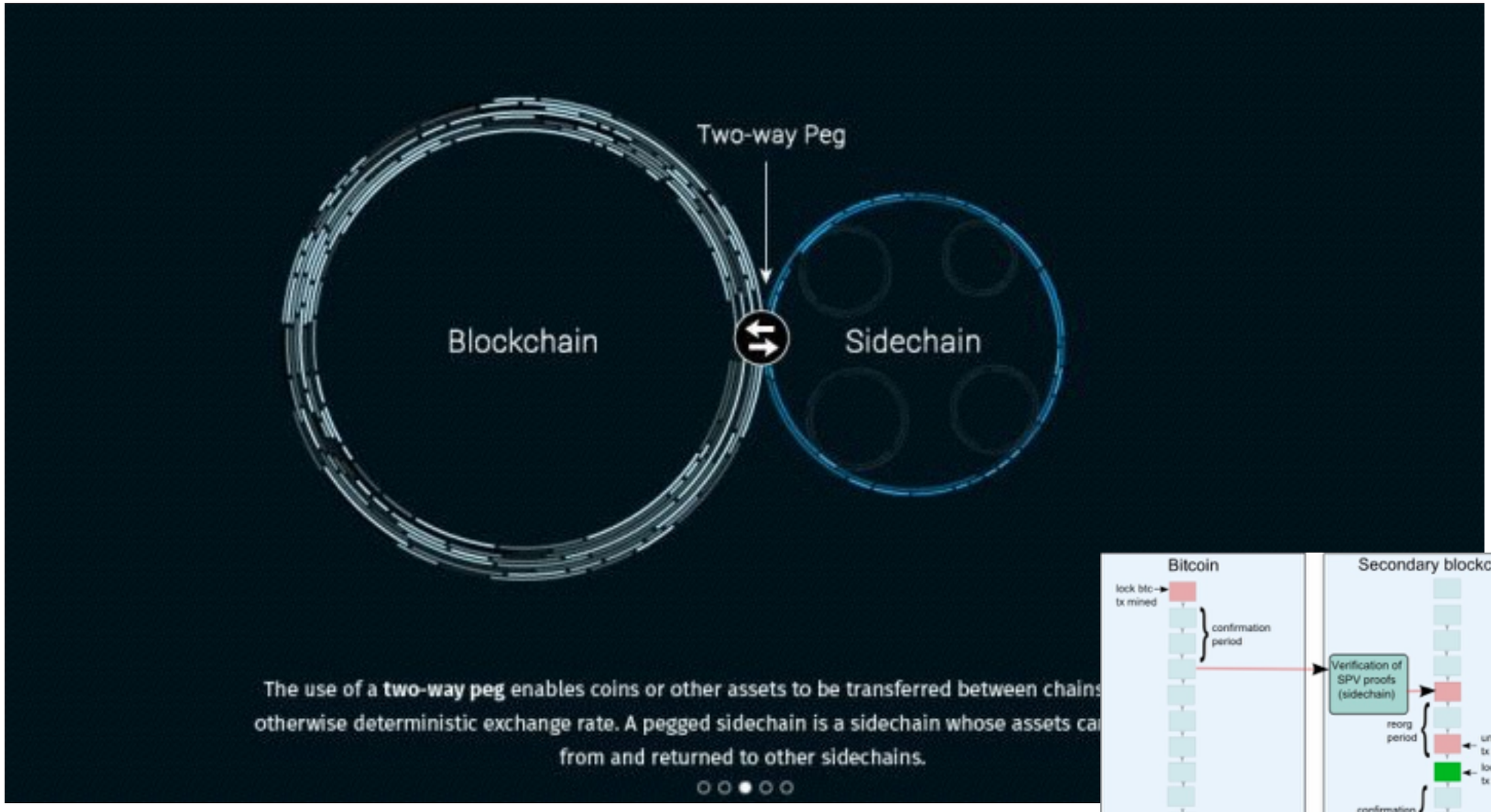


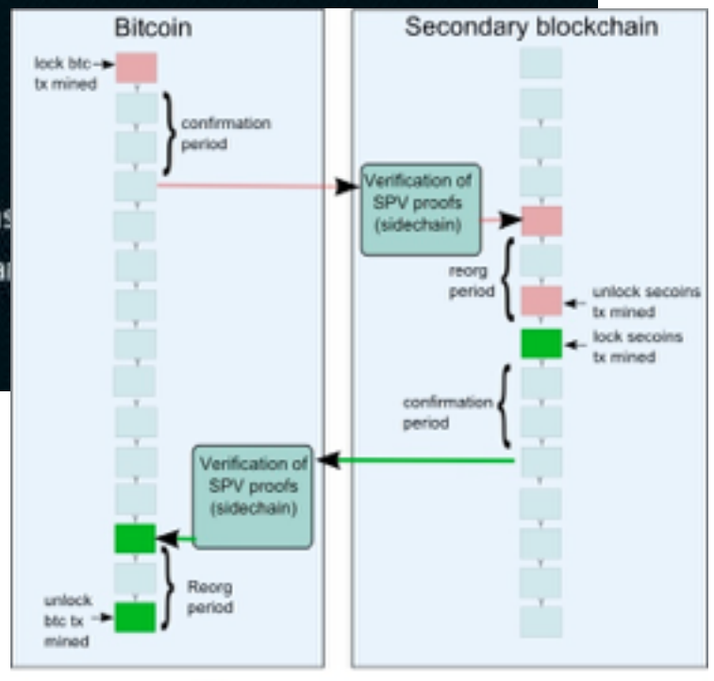
隔离见证

优点

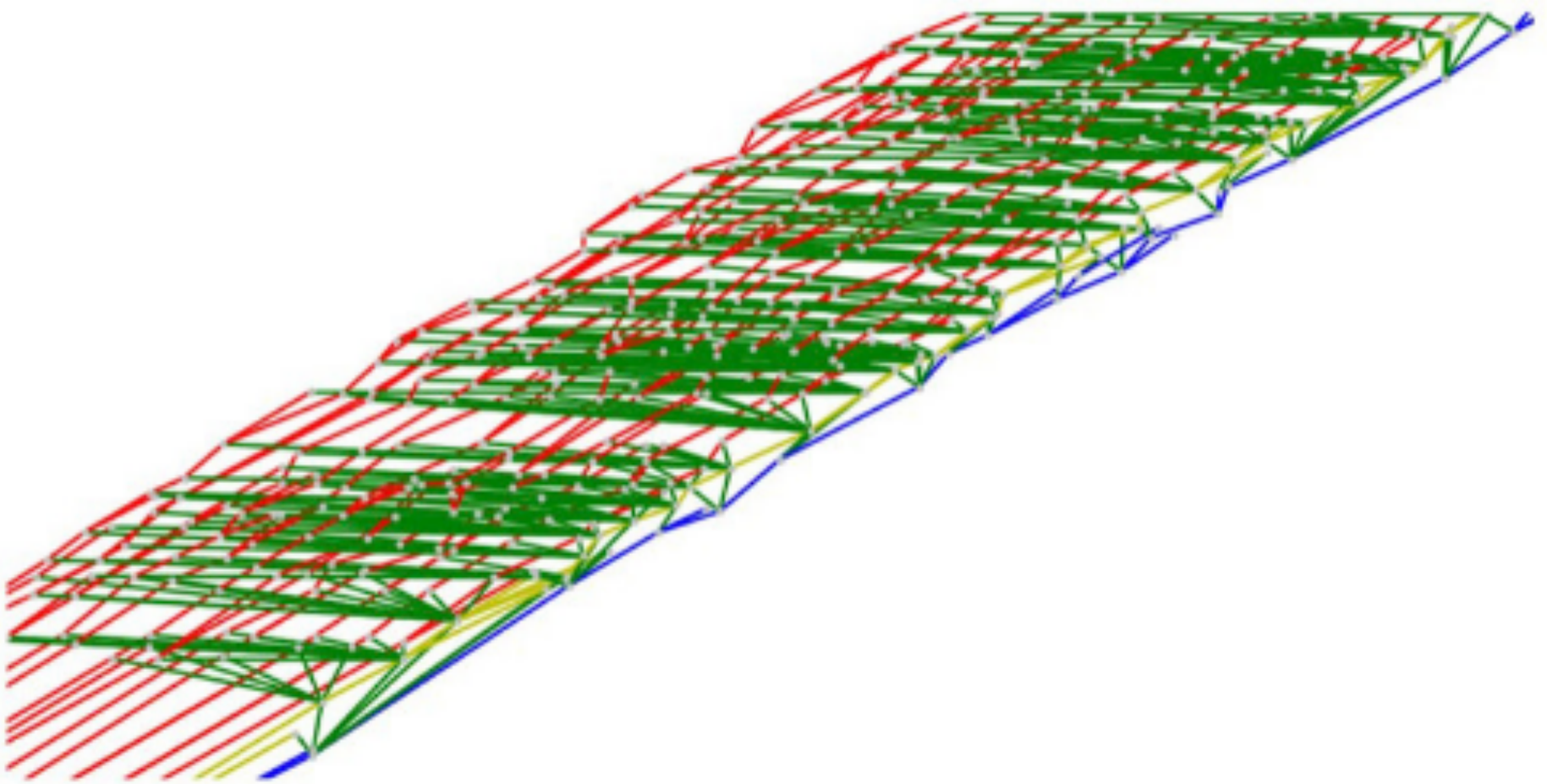
缺点

侧链

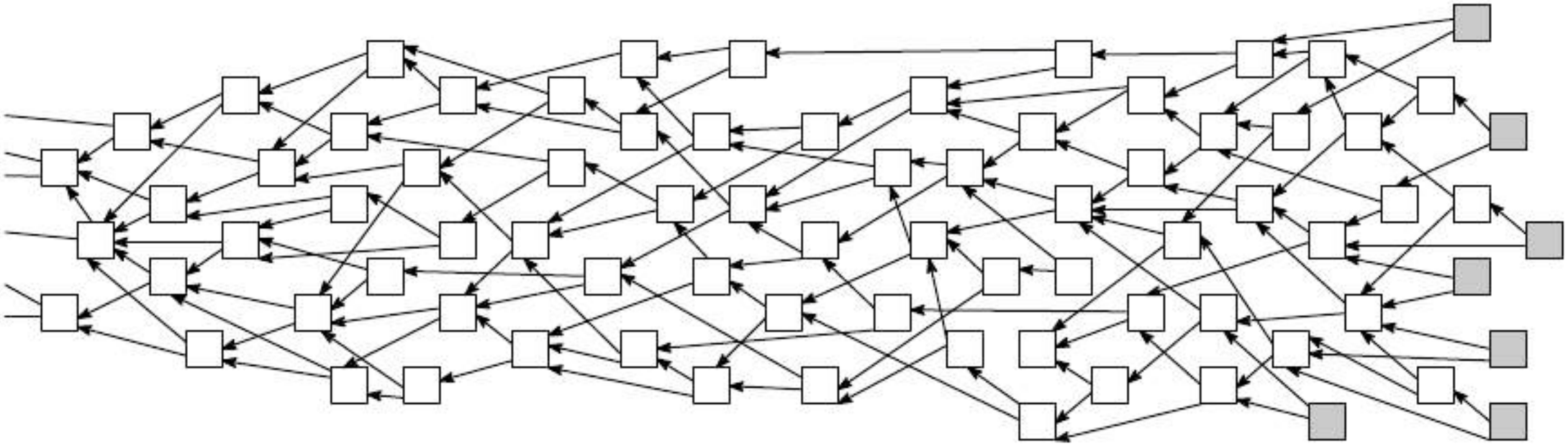

Two-way Peg
Blockchain
Sidechain
The use of a **two-way peg** enables coins or other assets to be transferred between chains
otherwise deterministic exchange rate. A pegged sidechain is a sidechain whose assets ca
from and returned to other sidechains.


Bitcoin
Secondary blockchain
lock btc tx mined
confirmation period
Verification of SPV proofs (sidechain)
reorg period
unlock secoins tx mined
lock secoins tx mined
confirmation period
Verification of SPV proofs (sidechain)
Reorg period
unlock btc tx mined
Affected blocks in secoins ->BTC transfer

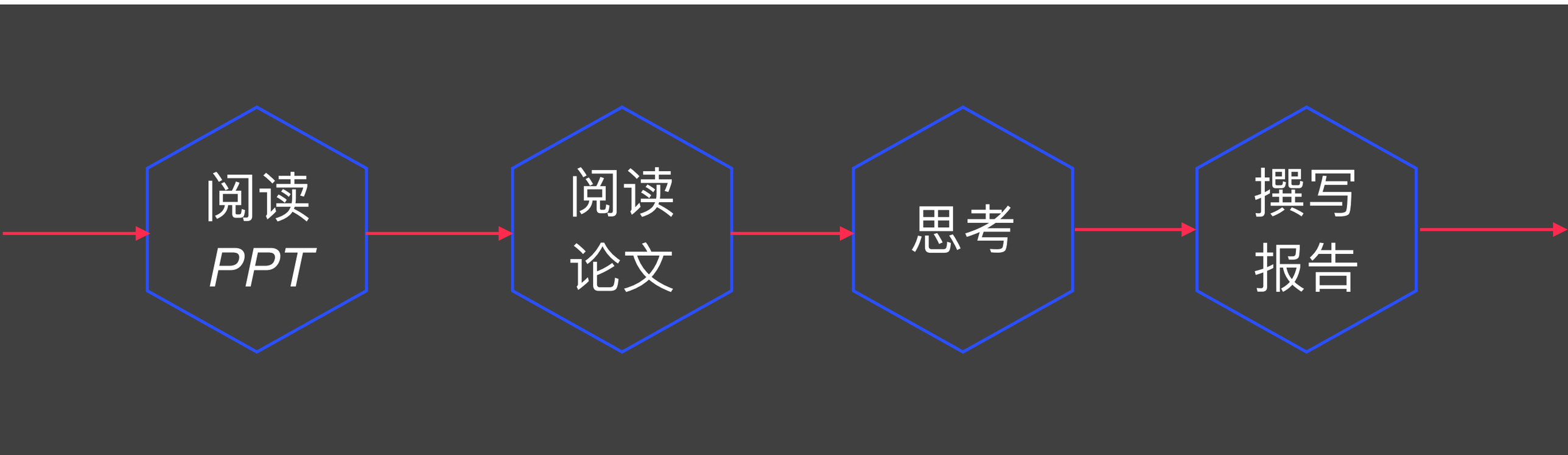
分片



DAG



课后作业



Homework

课后作业

要求阅读如下资料，写阅读报告

Bitcoin Developer Guide

Find detailed information about the Bitcoin protocol and related specifications.

https://bitcoin.org/en/developer-guide#block-chain-overview

1、资料概述

2、主要收获

3、存在疑问

4、所思所感

11月16日晚上12点前提交给助教

下节课20分钟测试，关于Bitcoin的

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