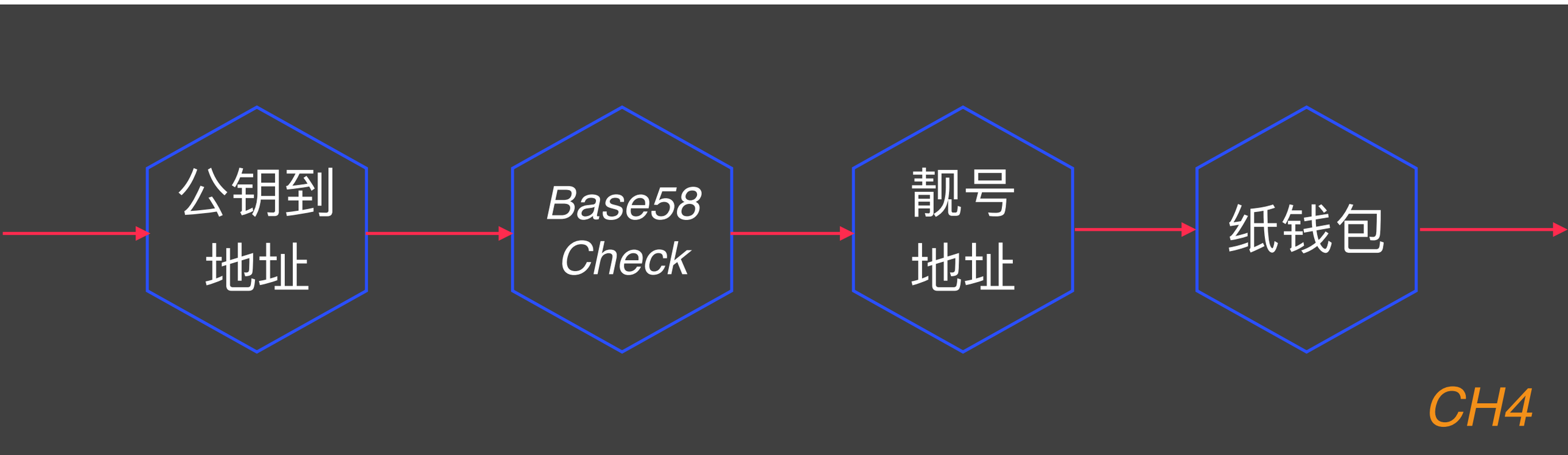
区块链

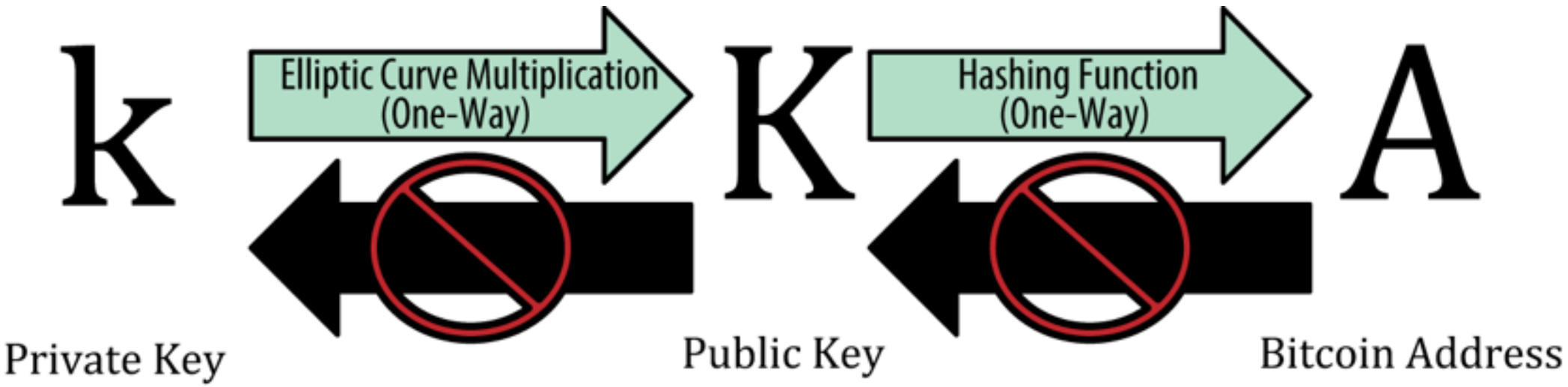
北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

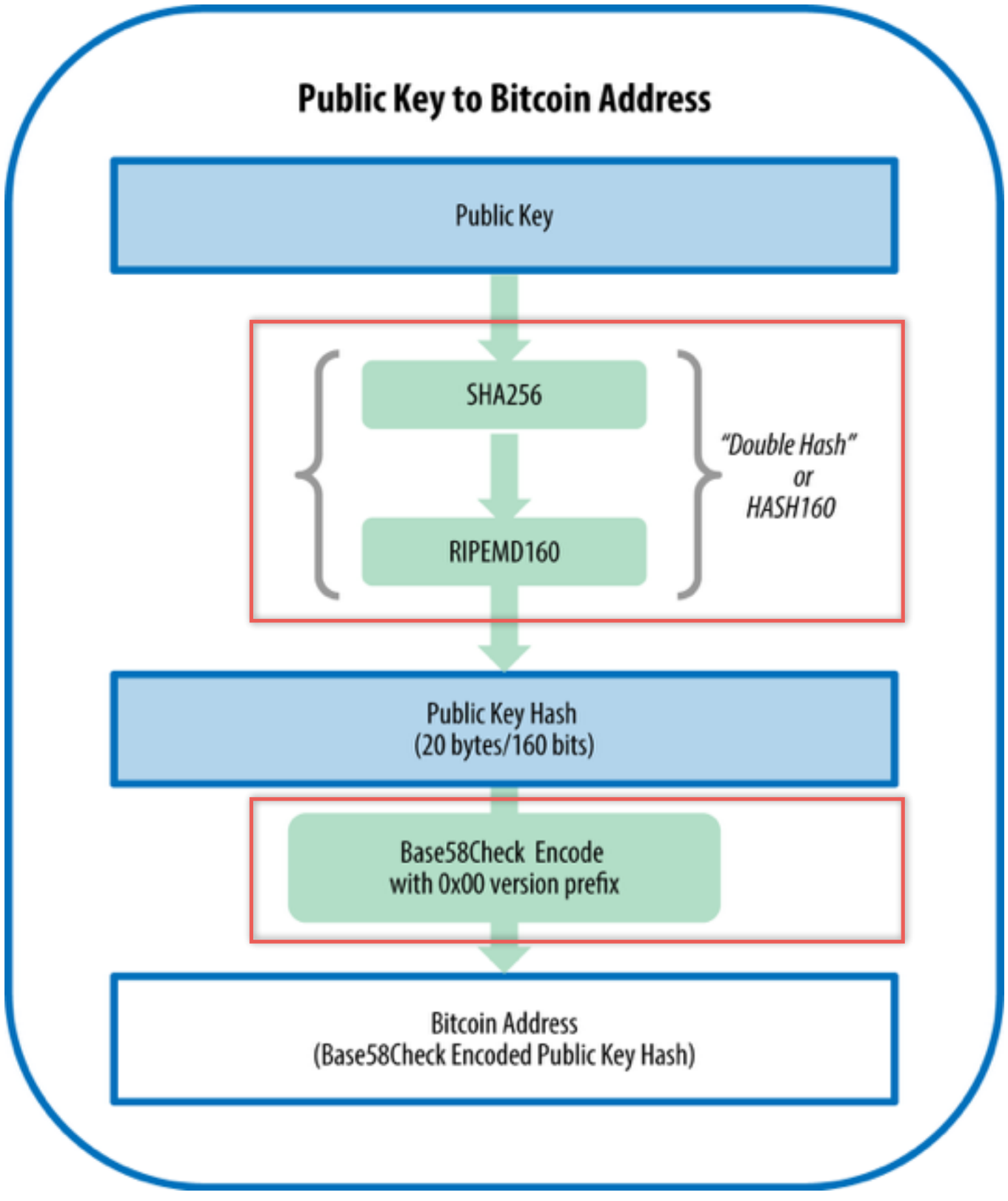
密钥和地址



私钥、公钥、地址


k
Elliptic Curve Multiplication
(One-Way)
K
Hashing Function
(One-Way)
A
Private Key
Public Key
Bitcoin Address

公钥到地址


Public Key to Bitcoin Address
Public Key
SHA256
RIPEMD160
"Double Hash"
or
HASH160
Public Key Hash
(20 bytes/160 bits)
Base58Check Encode
with 0x00 version prefix
Bitcoin Address
(Base58Check Encoded Public Key Hash)

Base58Check编码

Base64

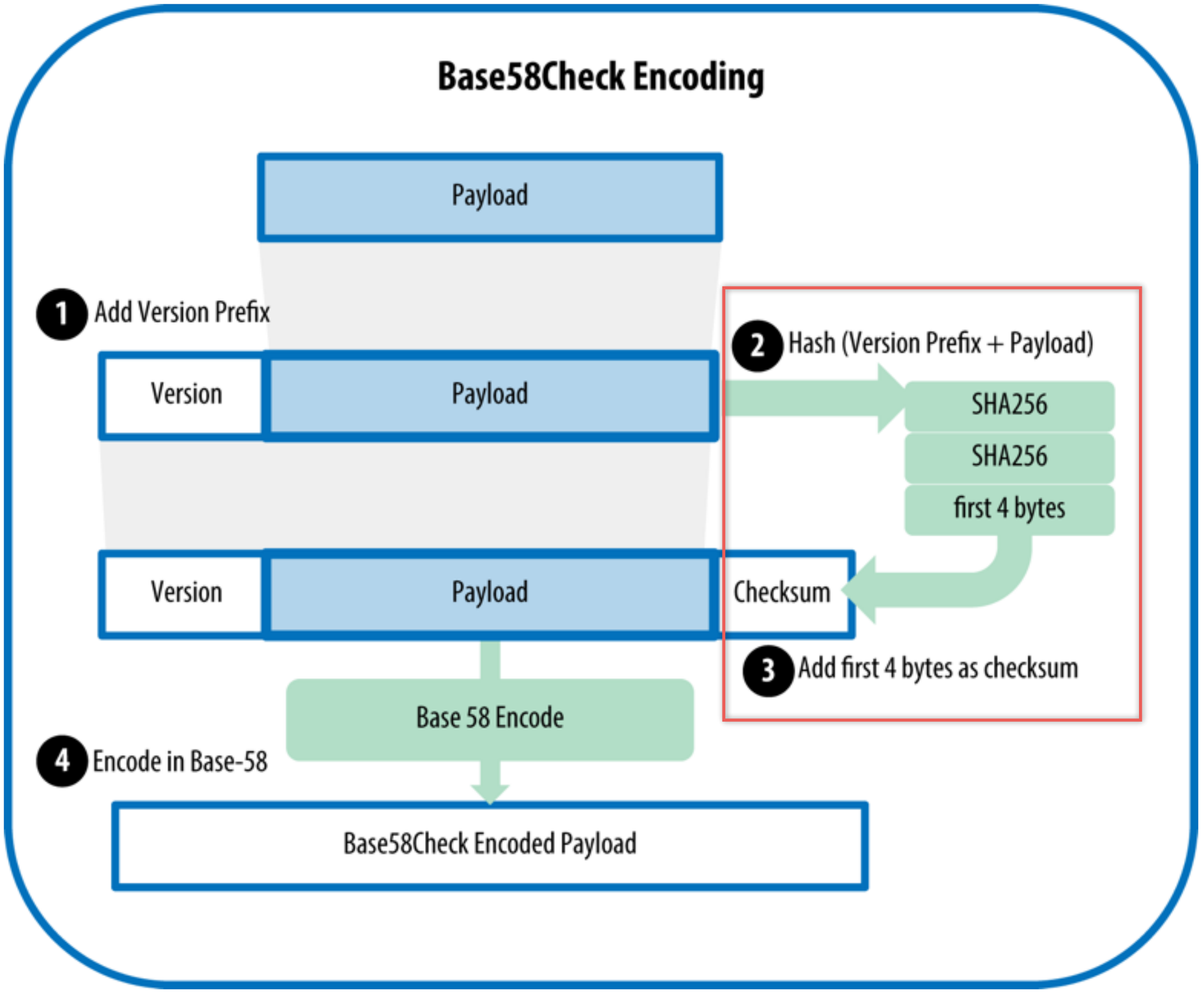
- 大写字母
- 小写字母
- 数字
- +、/

Base58

- 0和o
- I和l

Base58Check

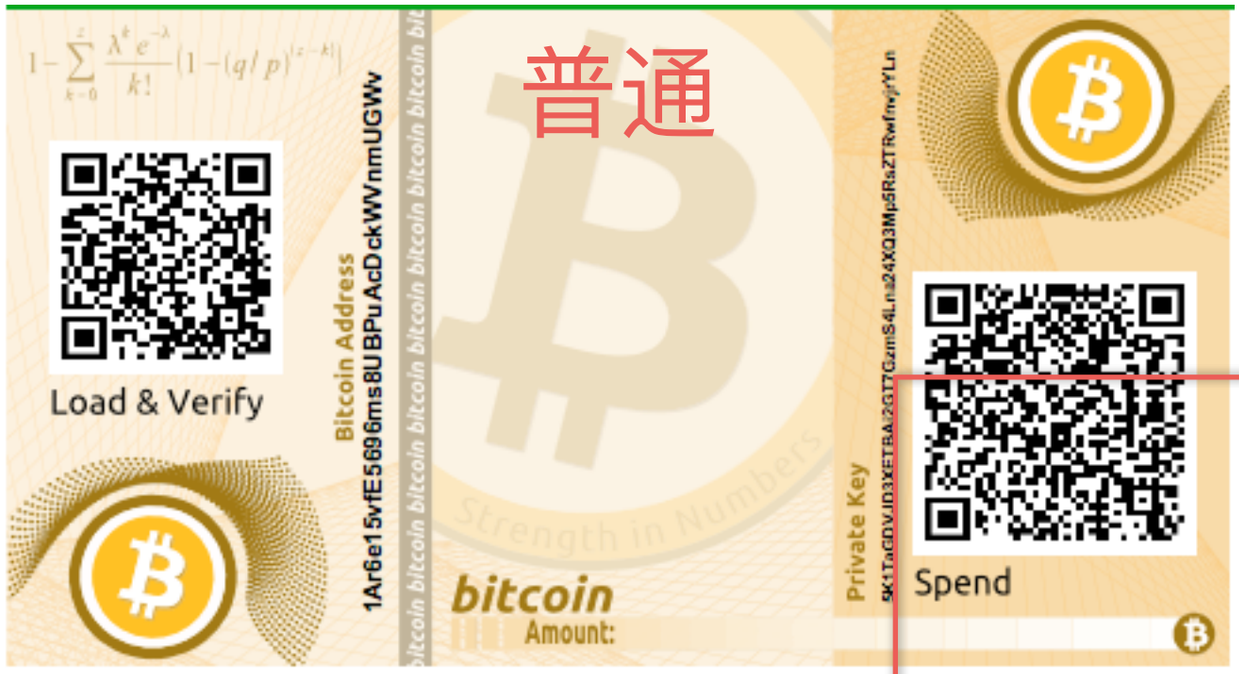
- 检验和

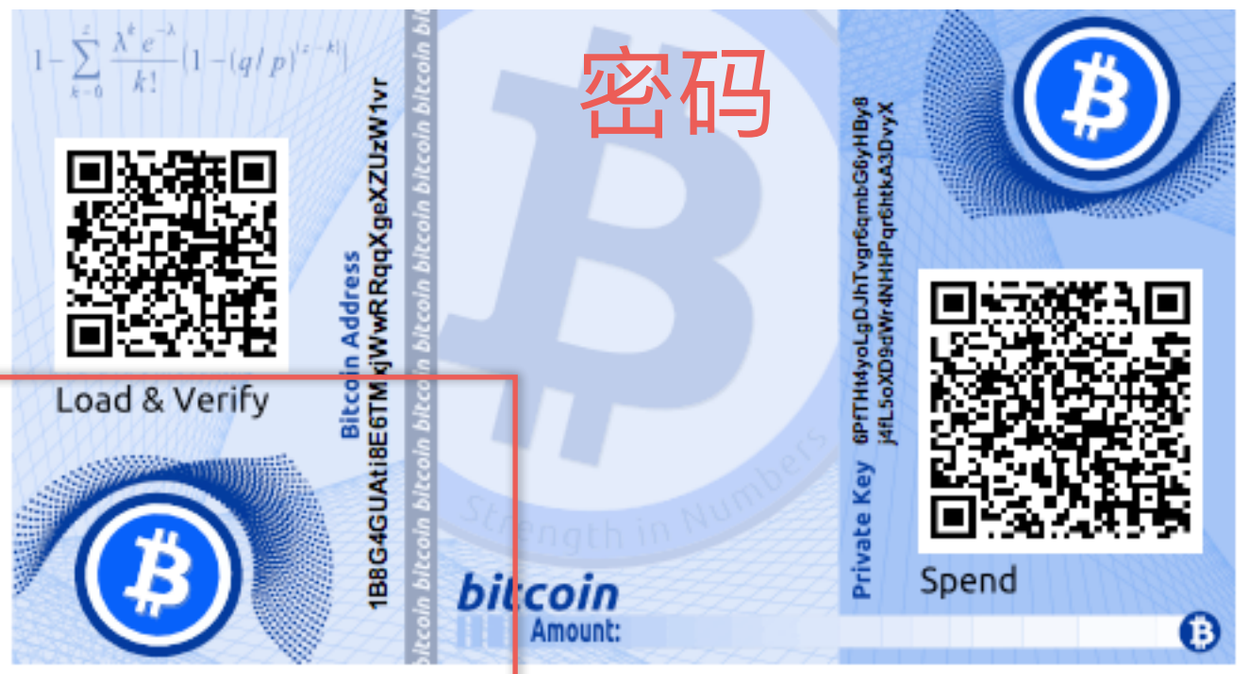


靓号地址

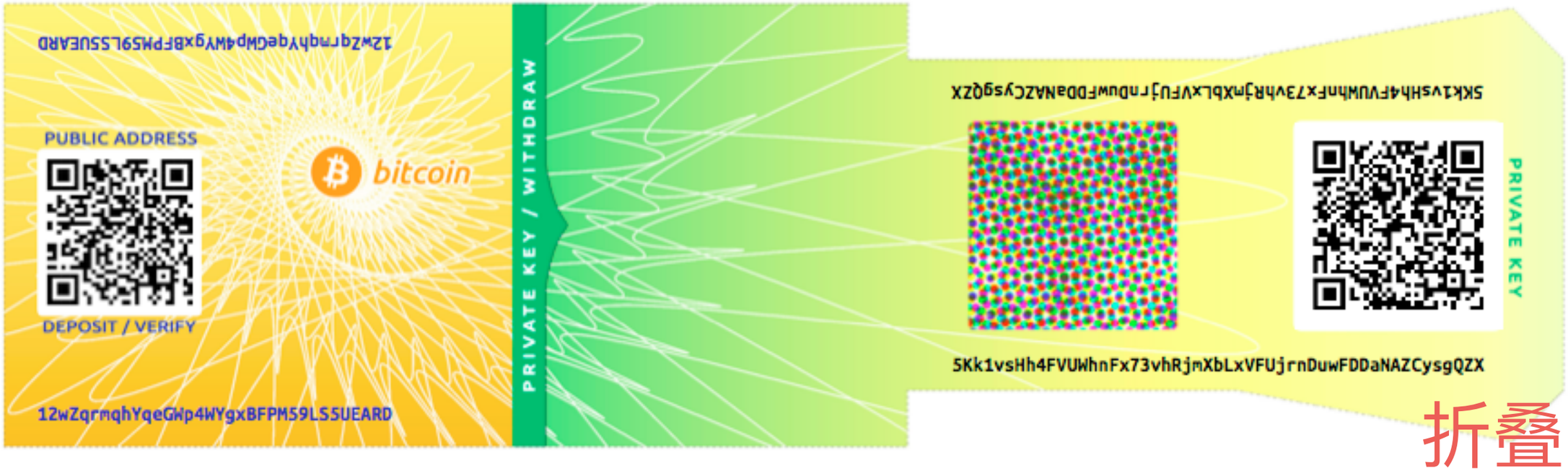
Length	Pattern	Frequency	Average search time
1	1K	1 in 58 keys	< 1 milliseconds
2	1Ki	1 in 3,364	50 milliseconds
3	1Kid	1 in 195,000	< 2 seconds
4	1Kids	1 in 11 million	1 minute
5	1KidsC	1 in 656 million	1 hour
6	1KidsCh	1 in 38 billion	2 days
7	1KidsCha	1 in 2.2 trillion	3–4 months
8	1KidsChar	1 in 128 trillion	13–18 years
9	1KidsChari	1 in 7 quadrillion	800 years
10	1KidsCharit	1 in 400 quadrillion	46,000 years
11	1KidsCharity	1 in 23 quintillion	2.5 million years

纸钱包





Public address	Private key (WIF)
1424C2F4bC9JidNjjTUZCbUxv6Sa1Mt62x	5J3mBbAH58CpQ3Y5RNJpUKPE62SQ5tfcvU2JpbnkeyhfsYB1Jcn



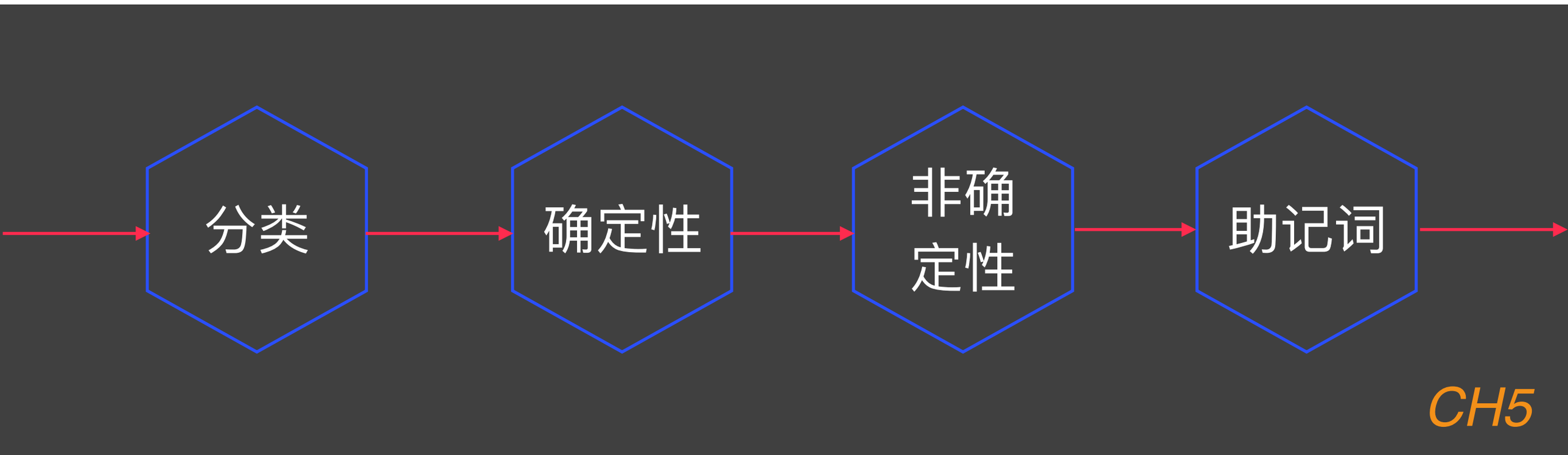
折叠

纸钱包

私钥
密封

多个副本

钱包



钱包

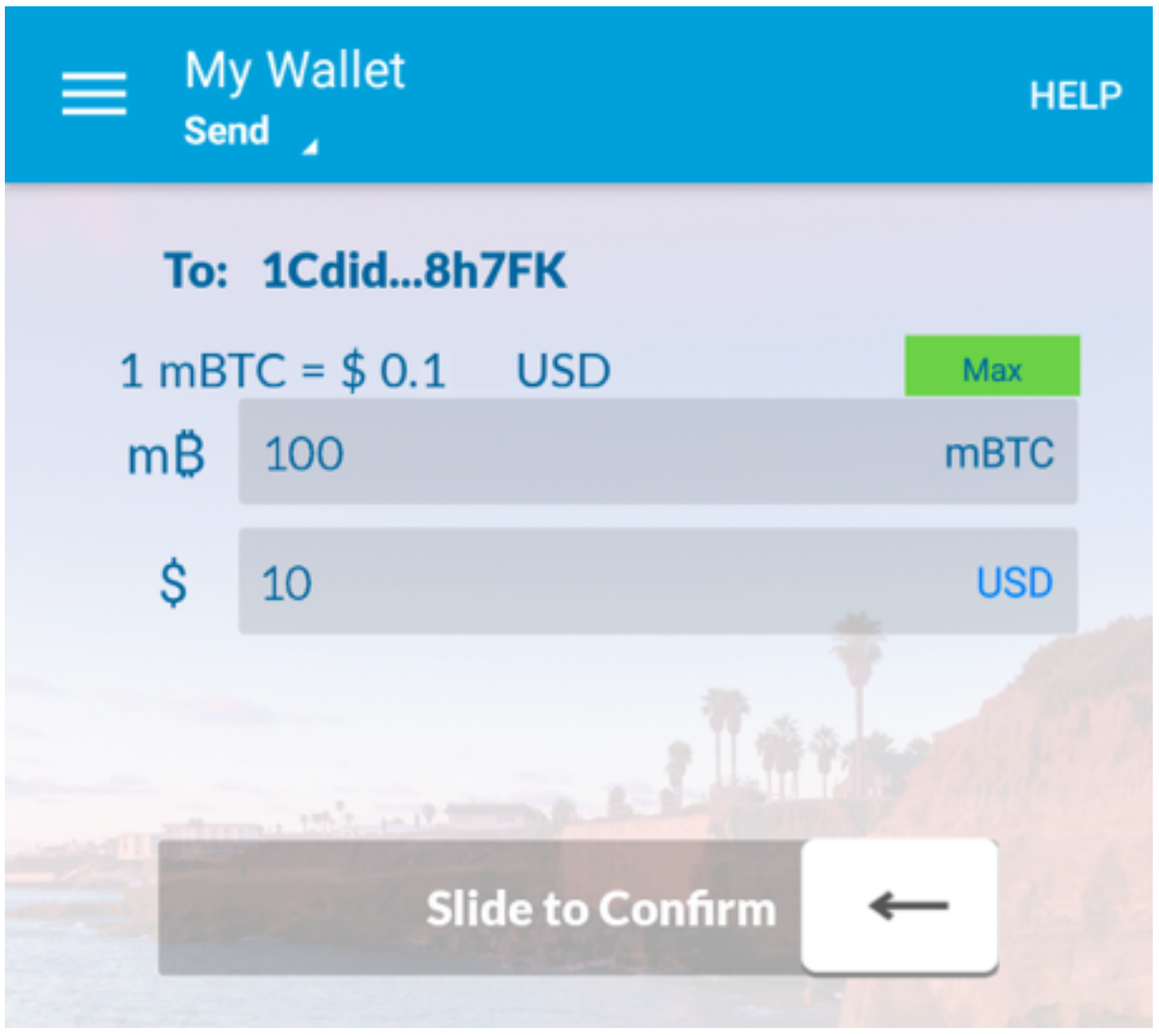
桌面钱包

手机钱包

网络钱包

硬件钱包

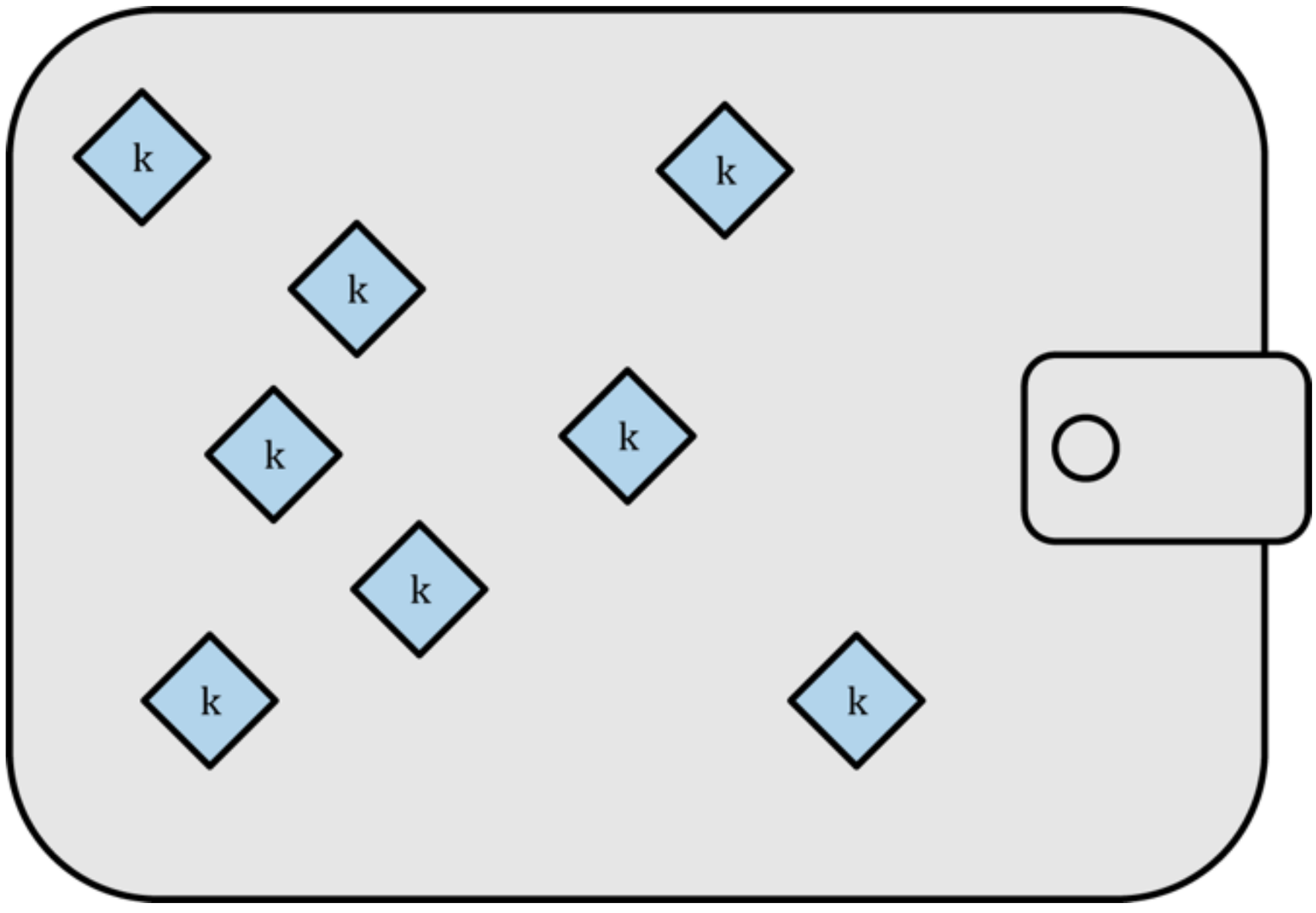
纸钱包



非确定性钱包

随机钱包

JBOK
Just a Bunch
of Keys

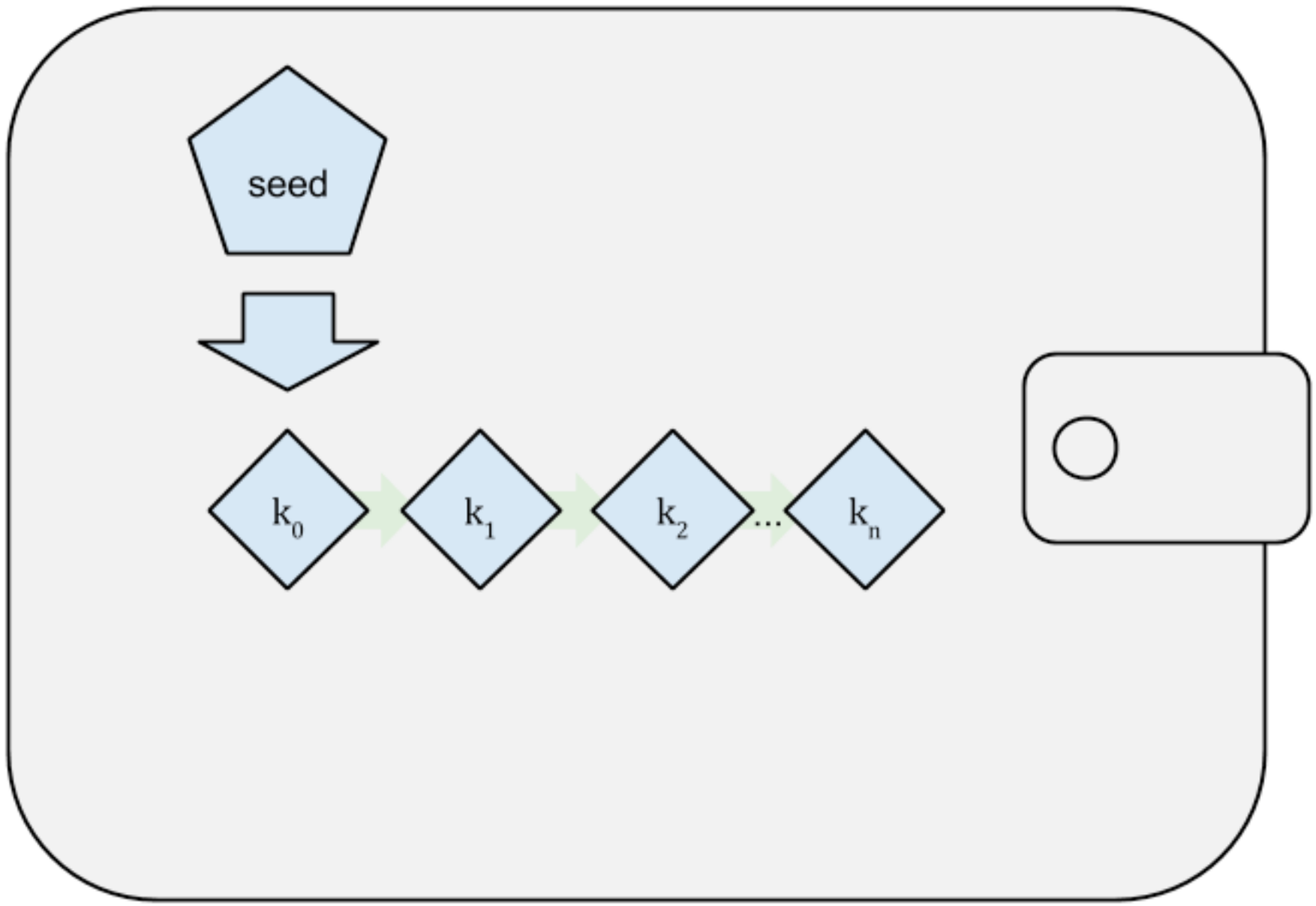


难于管理、
备份和导入

确定性钱包

种子钱包

种子
一串随机生成的数字

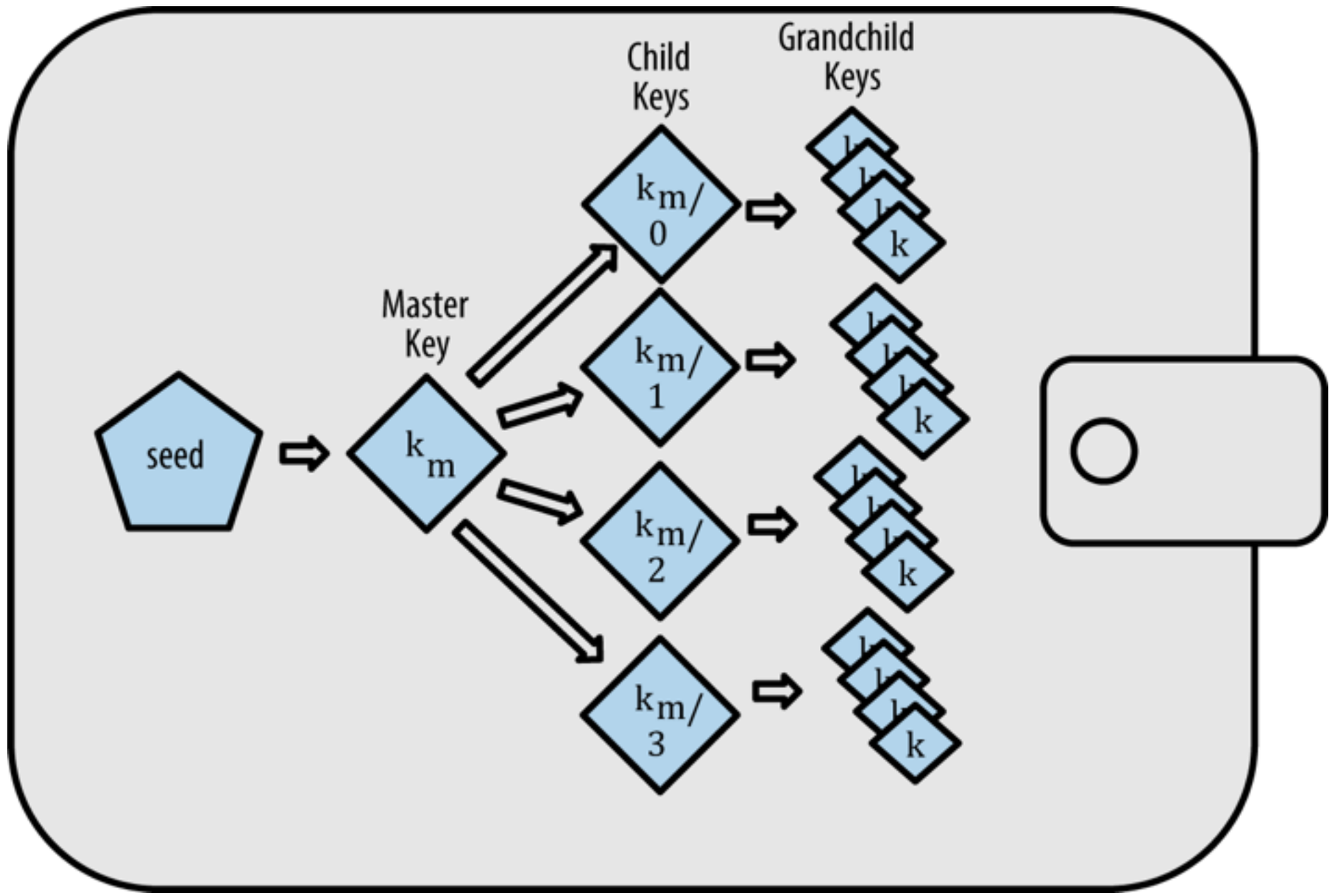


分层确定性钱包

HD钱包

BIP-32
BIP-43
BIP-44

BIP-39

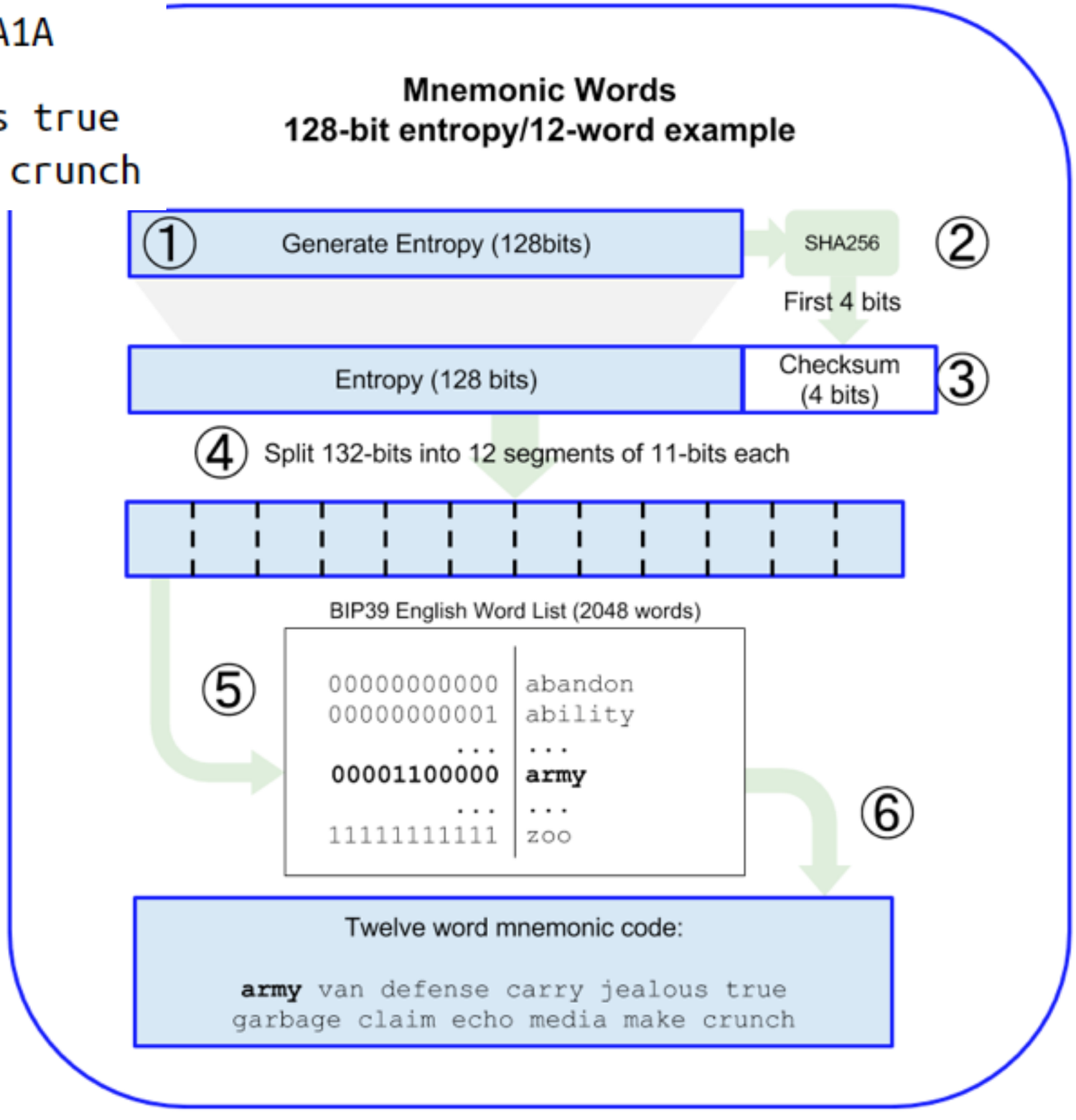


助记词

```
0C1E24E5917779D297E14D45F14E1A1A

army van defense carry jealous true
garbage claim echo media make crunch
```

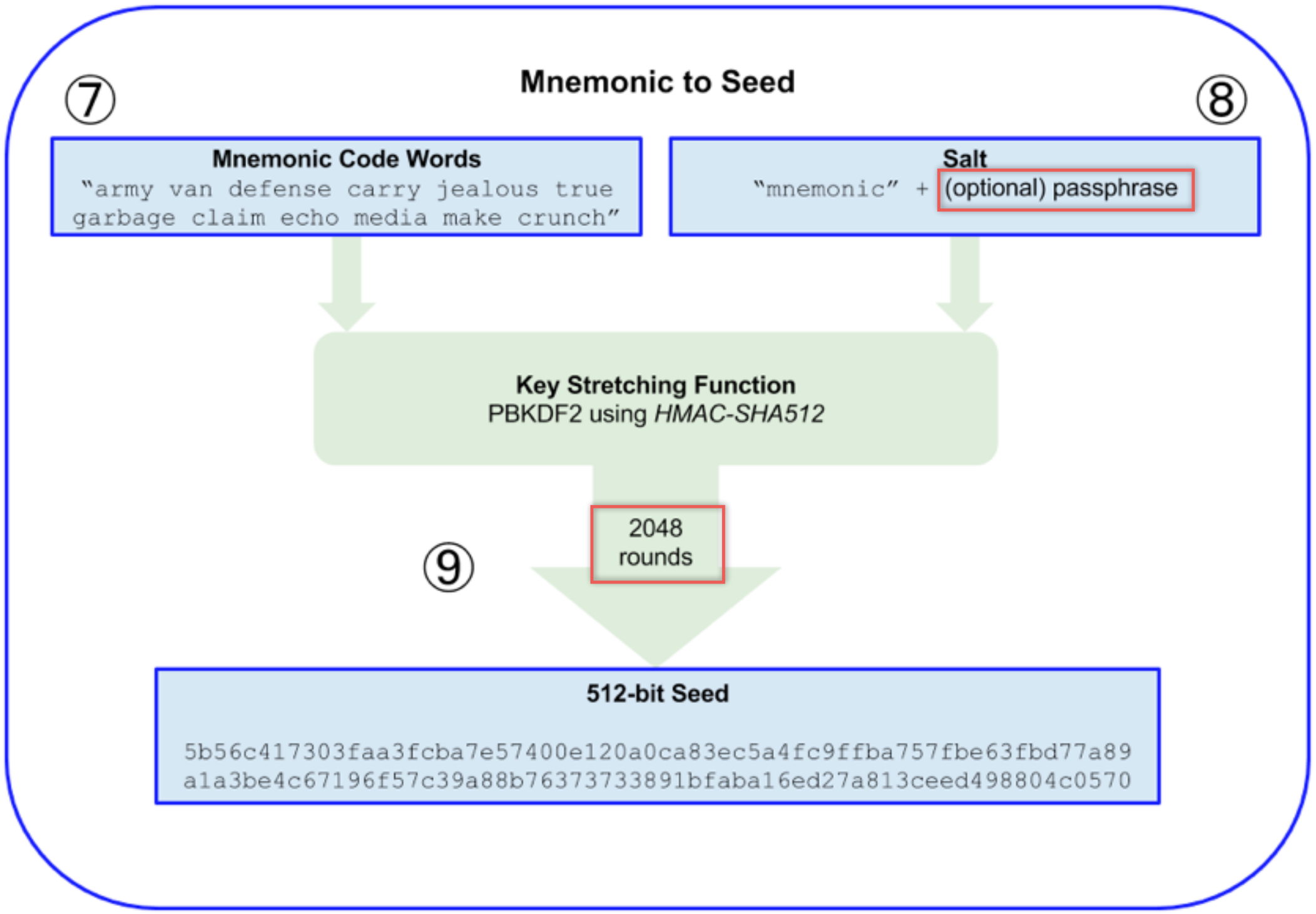
1. *army*
2. *van*
3. *defense*
4. *carry*
5. *jealous*
6. *true*
7. *garbage*
8. *claim*
9. *echo*
10. *media*
11. *make*
12. *crunch*



从助记词产生种子

密码延伸函数

PBKDF2



助记词

Mnemonic

You can enter an existing BIP39 mnemonic, or generate a new random one. Typing your own twelve words will probably not work how you expect, since the words require a particular structure (the last word is a checksum)

For more info see the BIP39 spec

Generate a random 12 word mnemonic, or enter your own below.

BIP39 Mnemonic

army van defense carry jealous true garbage claim echo media make crunch

BIP39 Passphrase (optional)

BIP39 Seed

5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fbd77a89a1a3be4c6719
6f57c39a88b76373733891bfaba16ed27a813ceed498804c0570

Coin

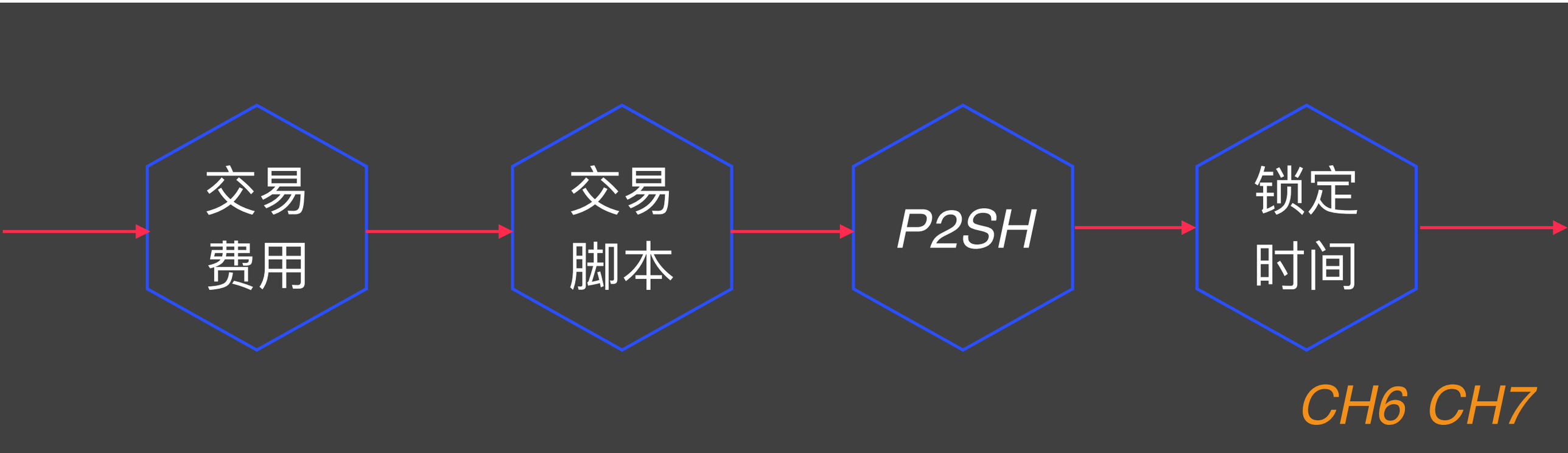
Bitcoin

BIP32 Root Key

xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6
i6ddYjb5PLtUdMZn8LhvuCVhGcQntq5rn7JVMqnie

https://iancoleman.io/bip39/

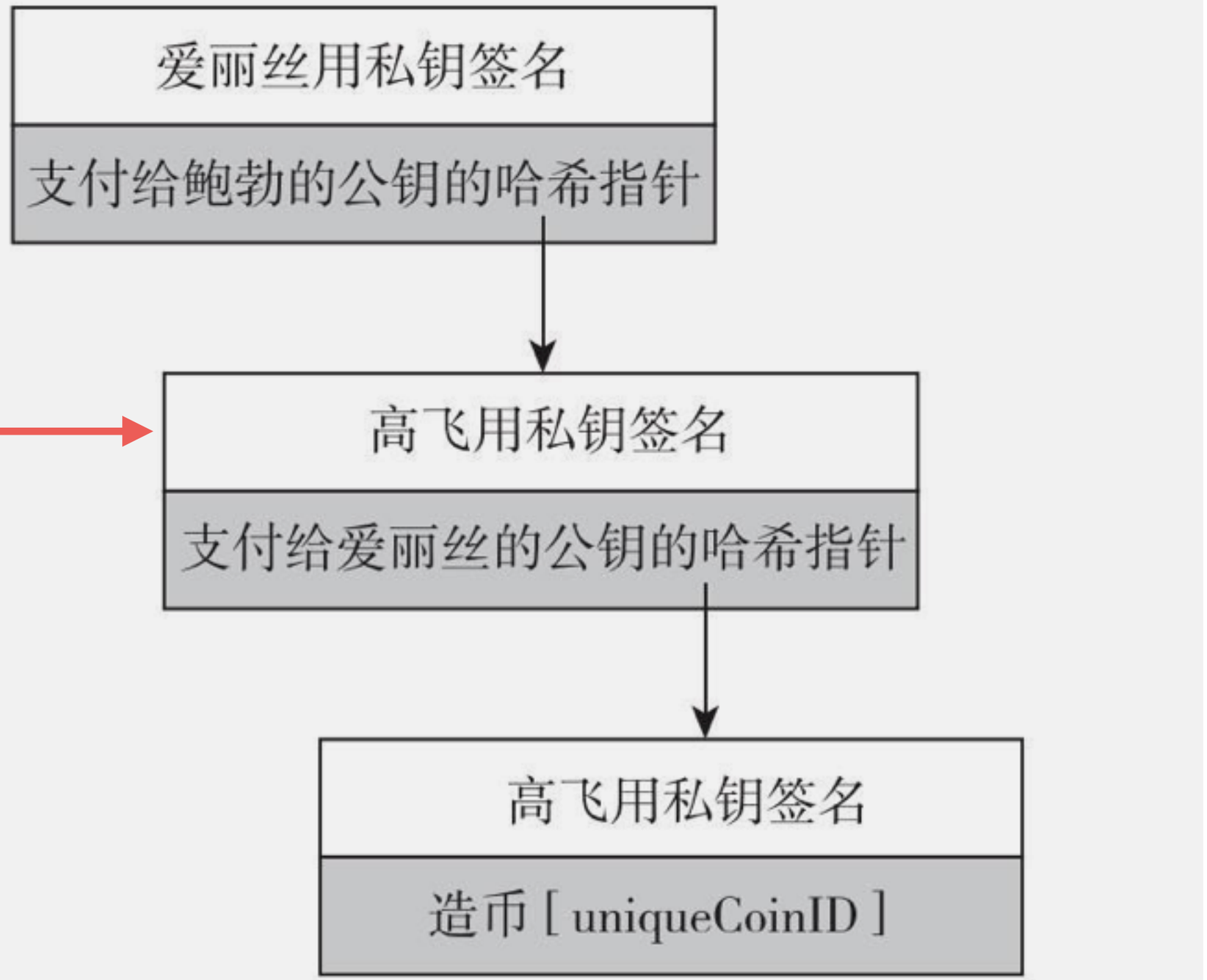
交易



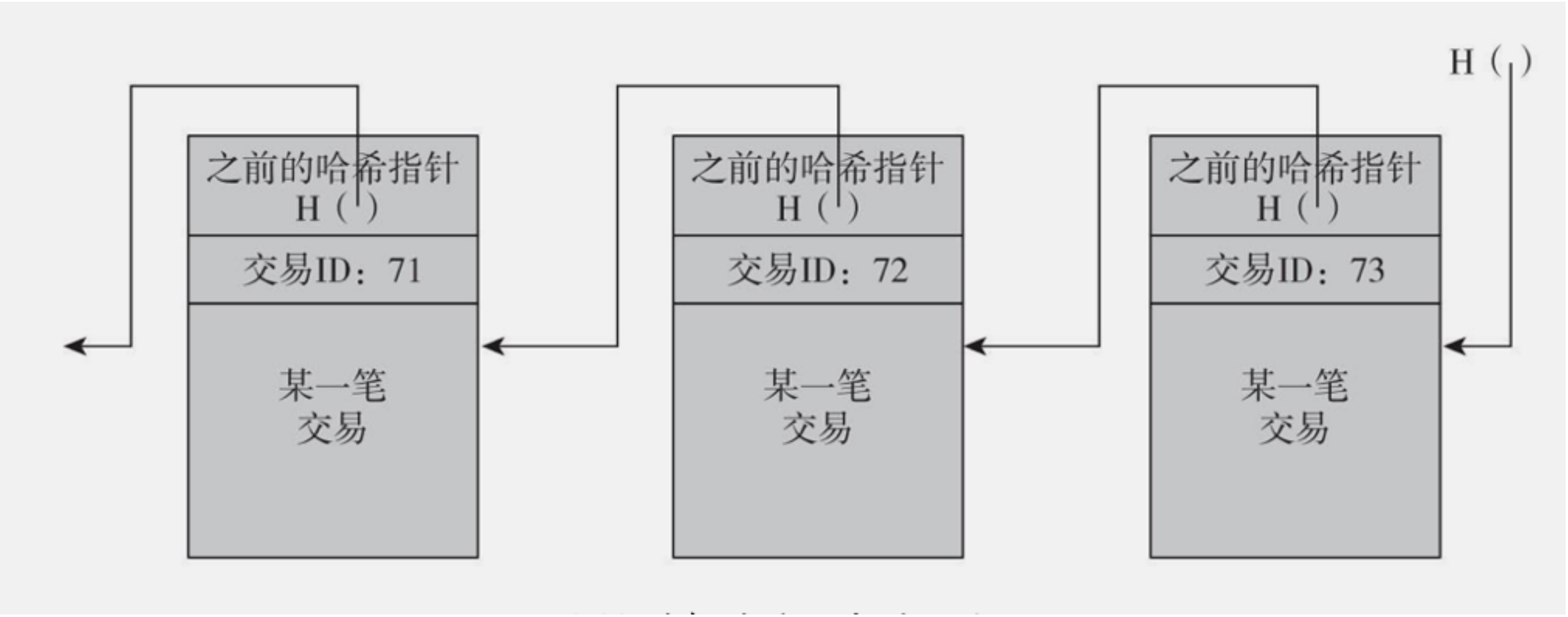
高飞币

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

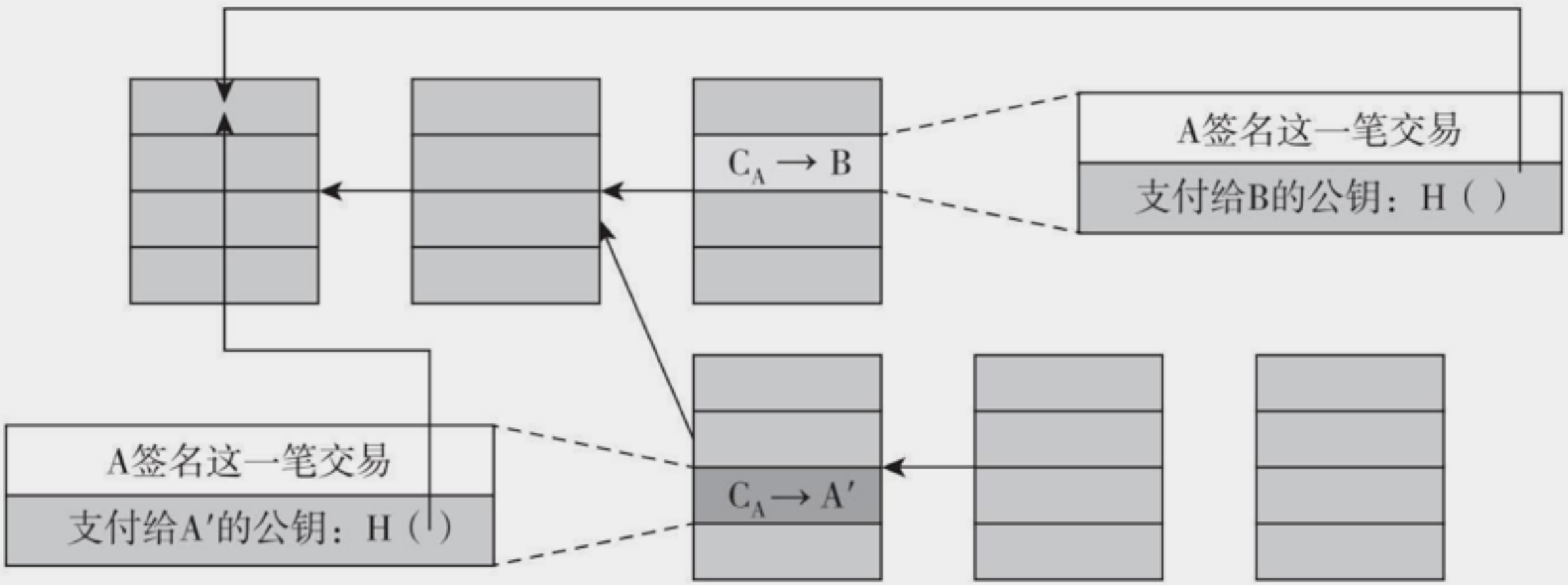


图2.2 双重支付攻击

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

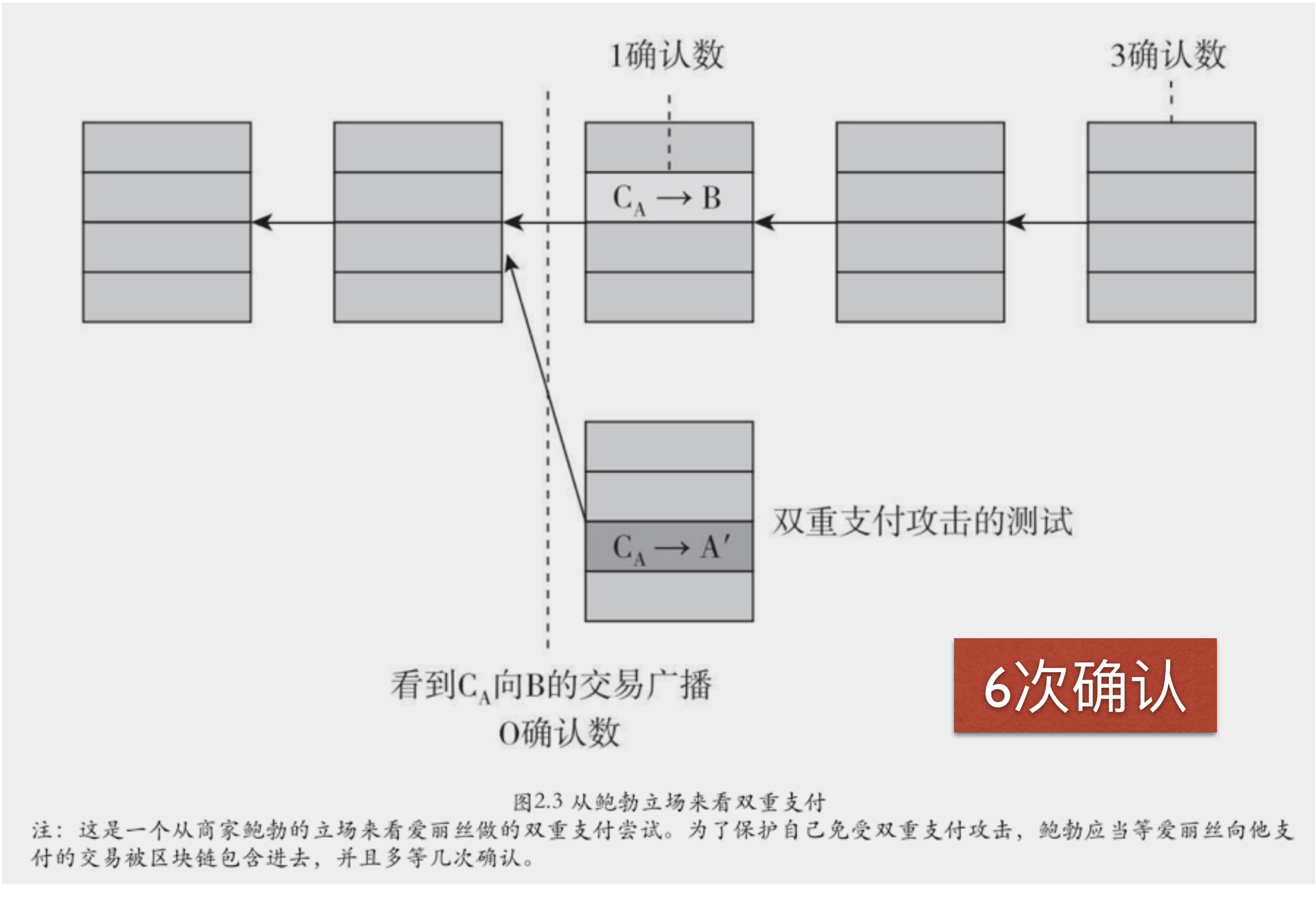
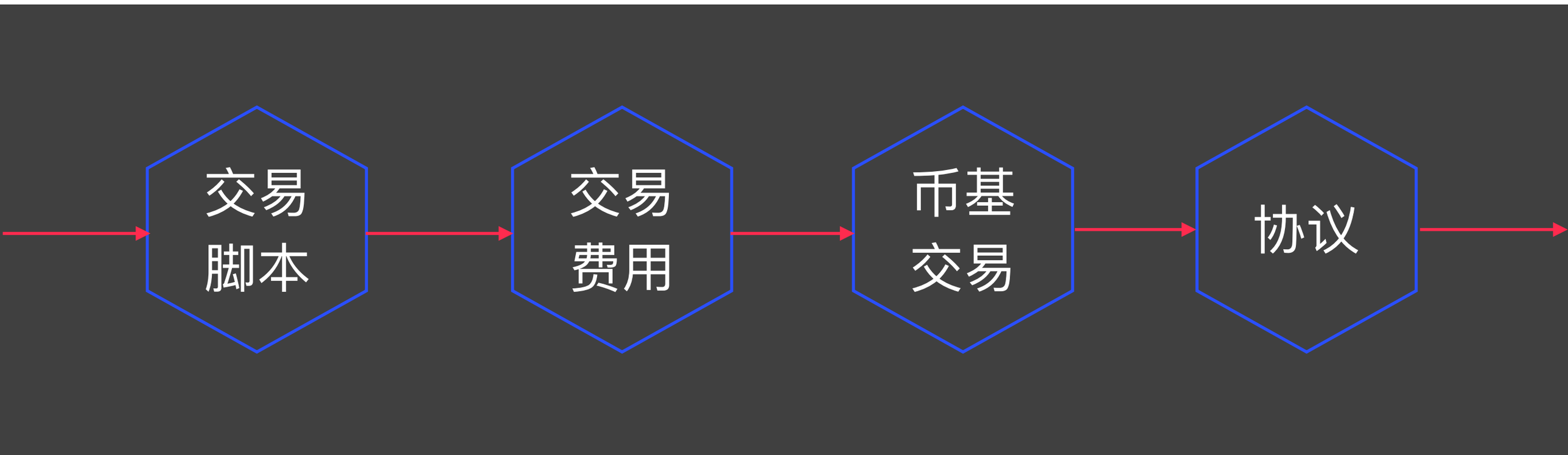


图2.3 从鲍勃立场来看双重支付

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。

交易



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
```

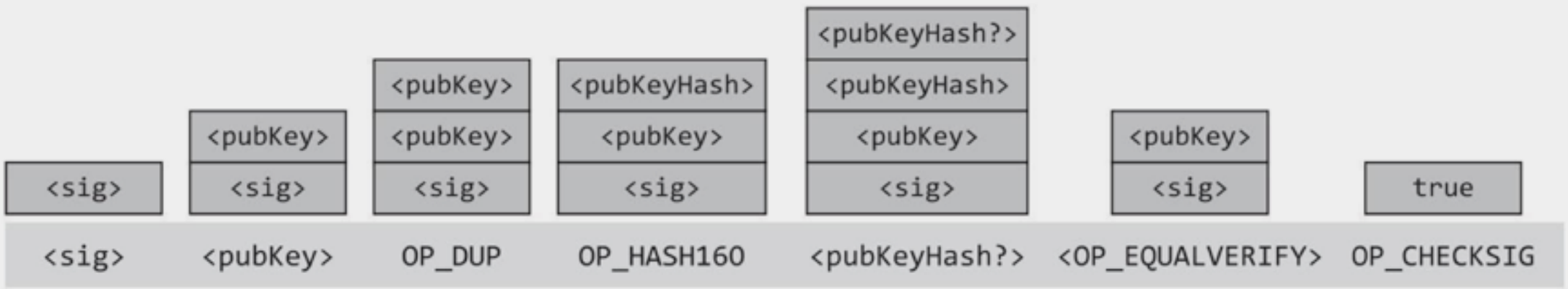
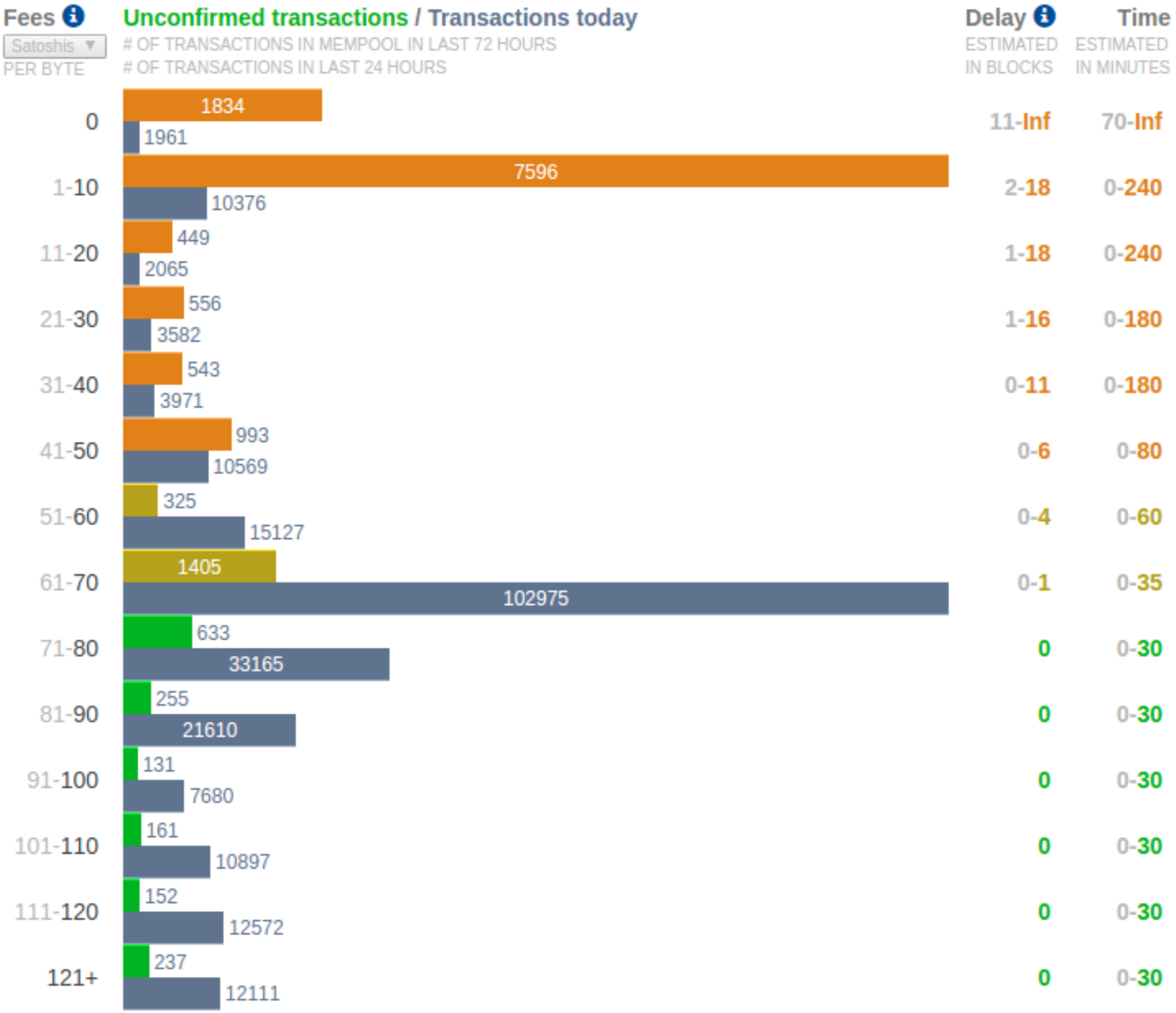


图3.6 比特币脚本的执行堆栈状态图

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。

交易费用


Fees
Satoshis
PER BYTE
Unconfirmed transactions / Transactions today
OF TRANSACTIONS IN MEMPOOL IN LAST 72 HOURS
OF TRANSACTIONS IN LAST 24 HOURS
Delay
ESTIMATED IN BLOCKS
Time
ESTIMATED IN MINUTES
0 1834 1961 11-Inf 70-Inf
1-10 7596 10376 2-18 0-240
11-20 449 2065 1-18 0-240
21-30 556 3582 1-16 0-180
31-40 543 3971 0-11 0-180
41-50 993 10569 0-6 0-80
51-60 325 15127 0-4 0-60
61-70 1405 102975 0-1 0-35
71-80 633 33165 0 0-30
81-90 255 21610 0 0-30
91-100 131 7680 0 0-30
101-110 161 10897 0 0-30
111-120 152 12572 0 0-30
121+ 237 12111 0 0-30

比特币交易程序

元数据

输入

输出

```
{
  "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"
   }
  ]
}
```

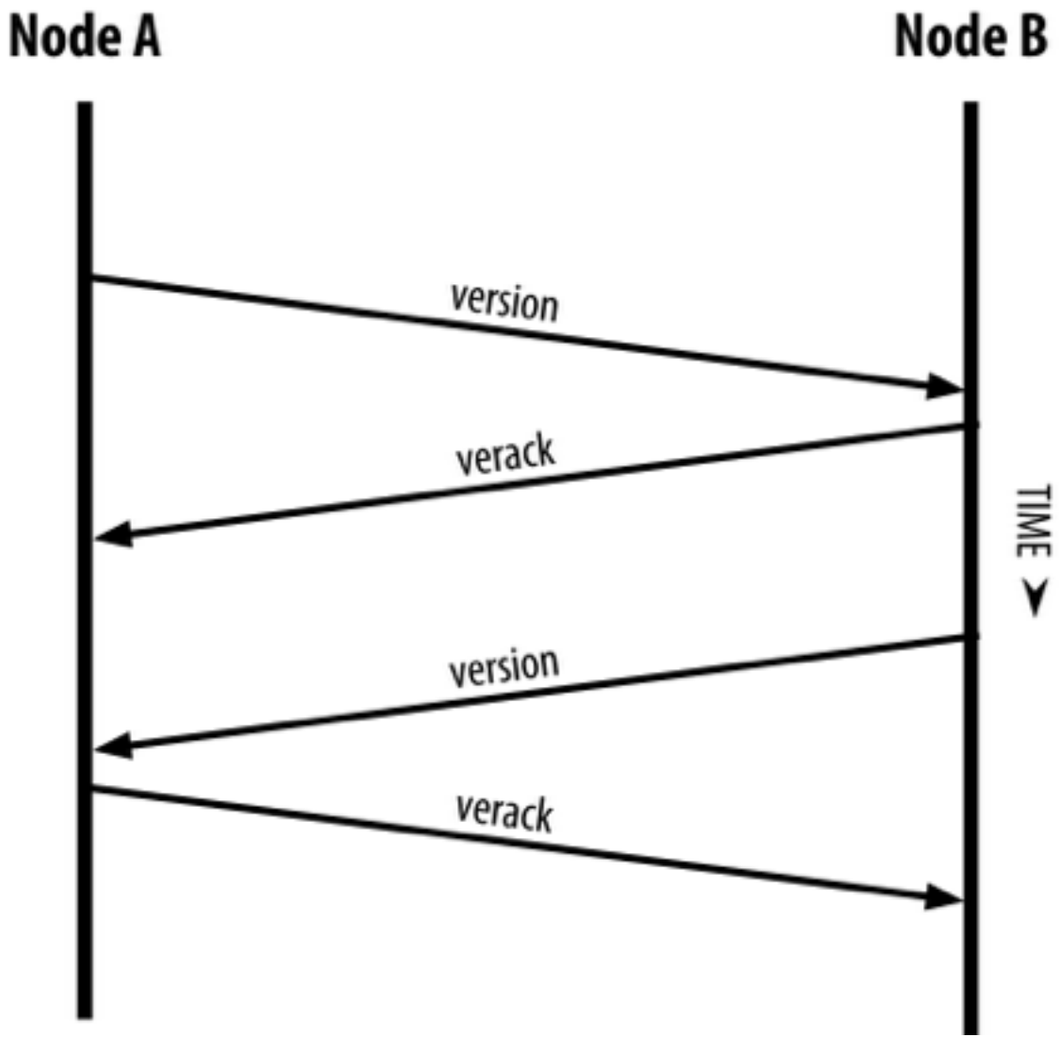
图3.3 一个真实的比特币交易程序段

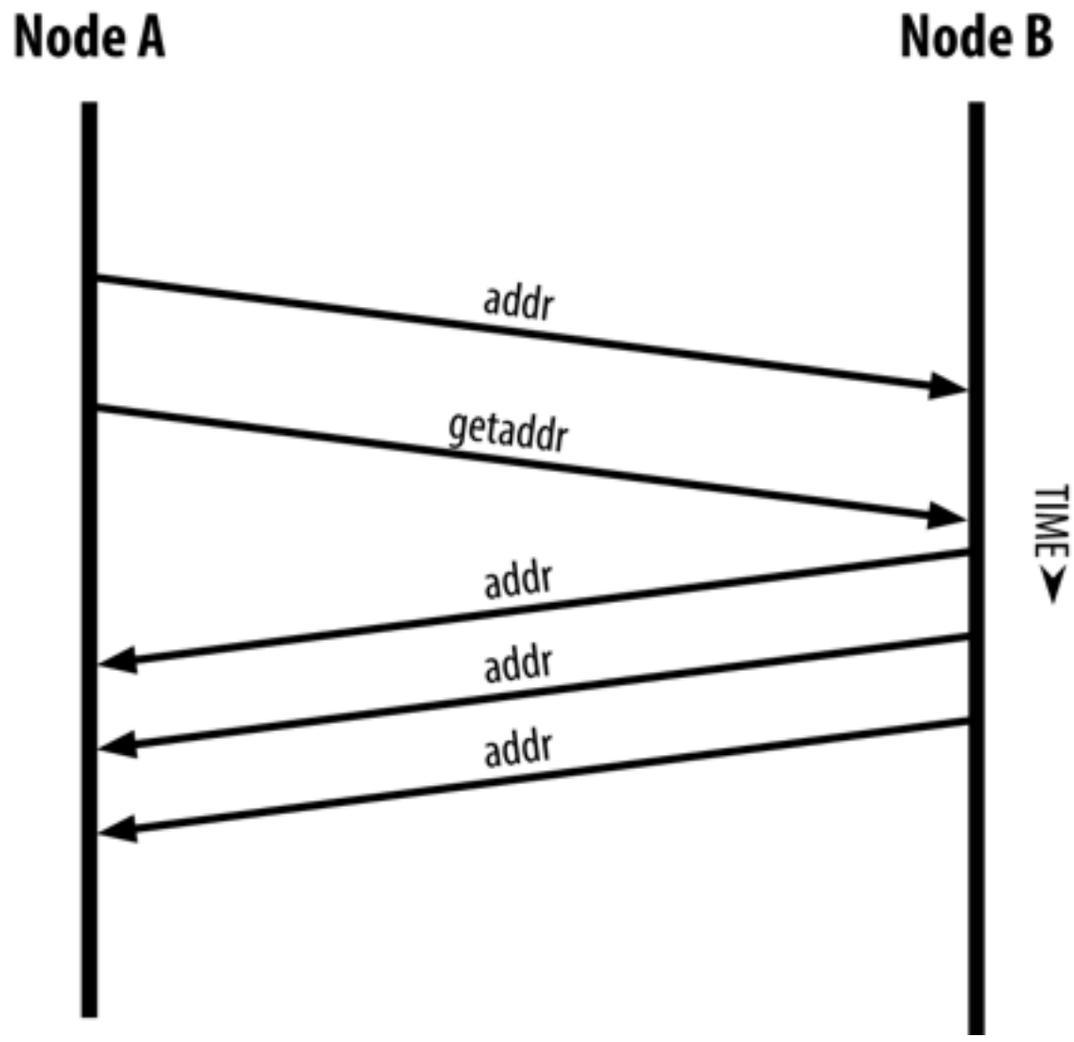
币基交易

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

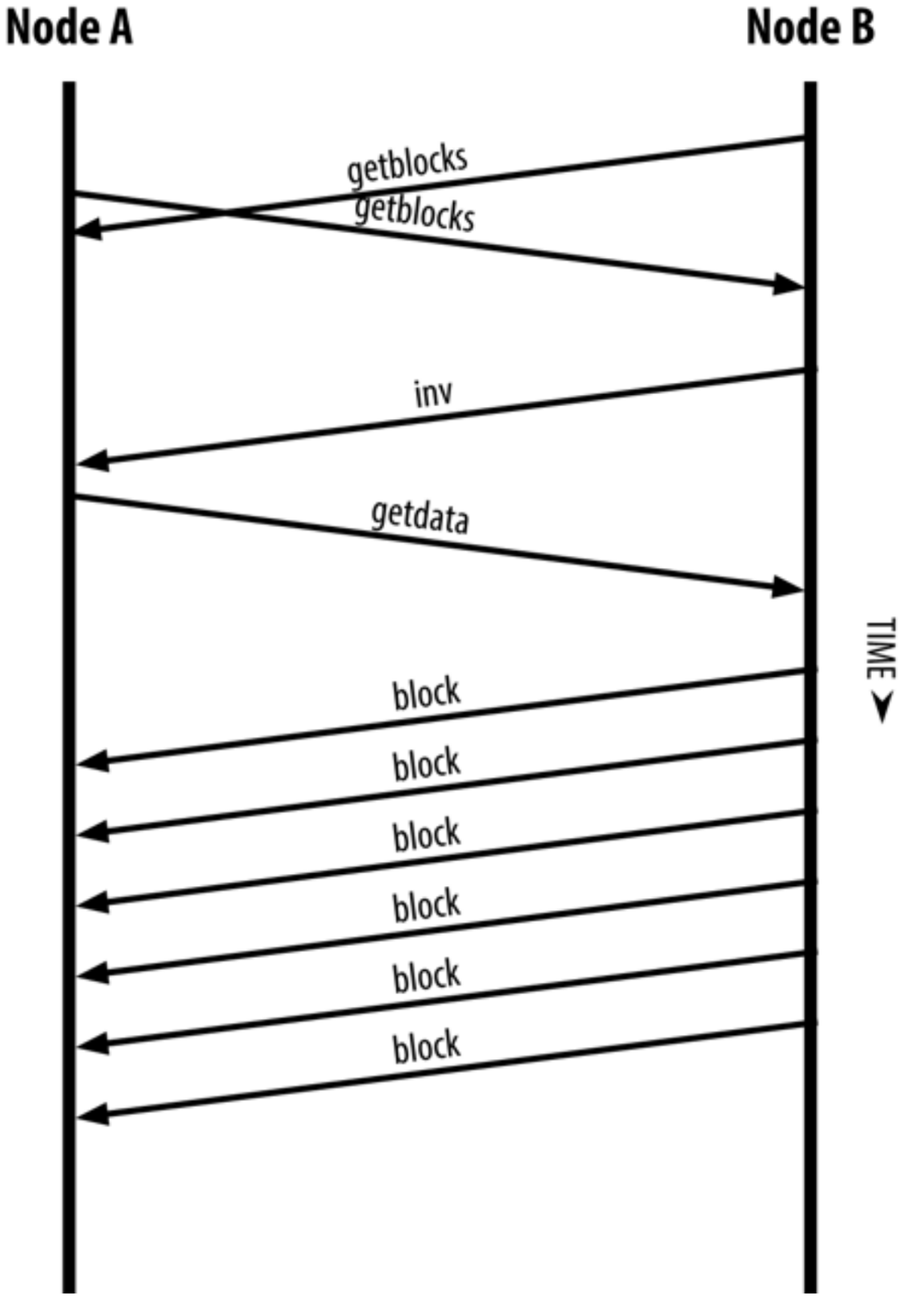
图3.8 币基交易

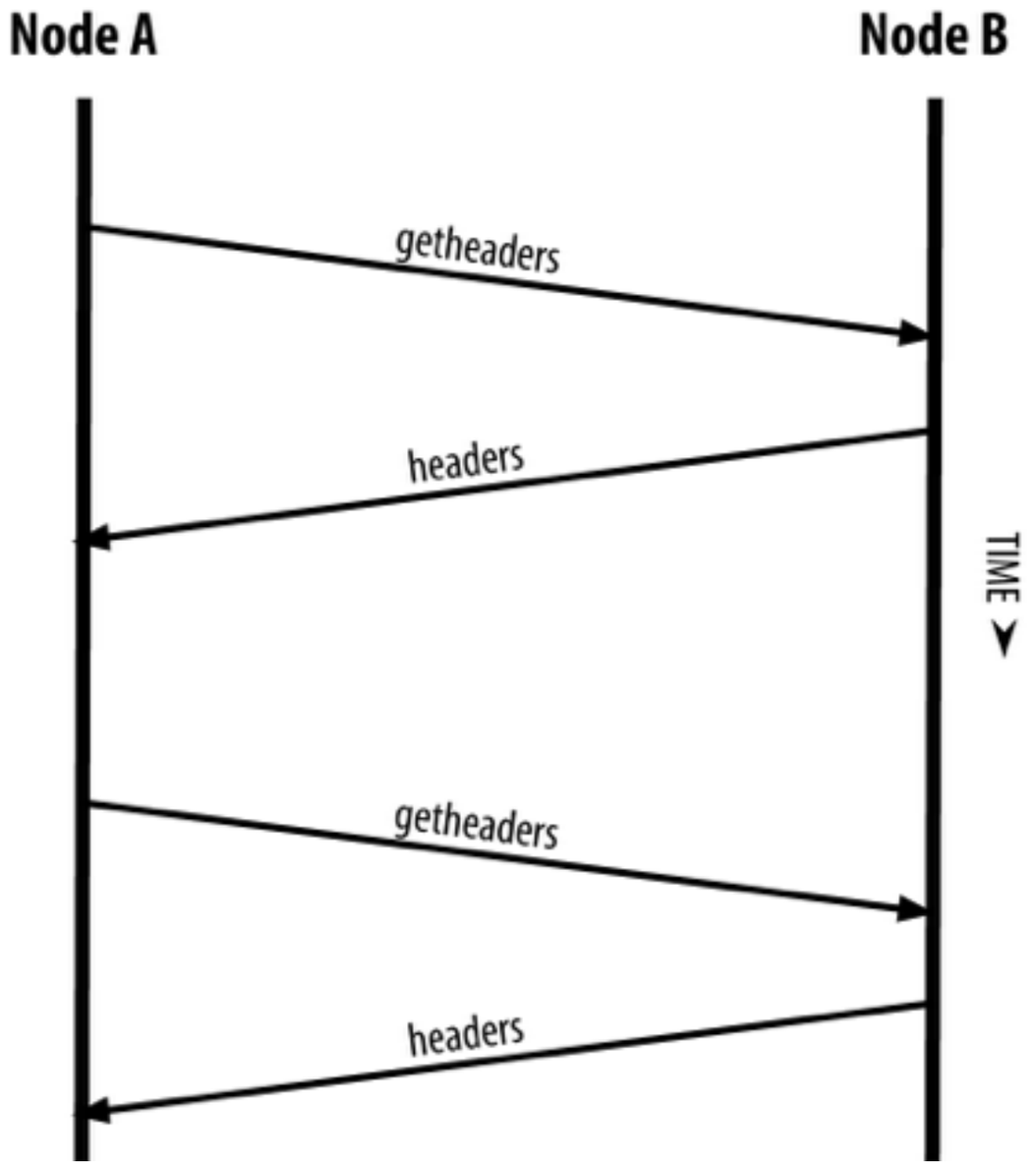
协议


Node A
Node B
version
verack
TIME
version
verack

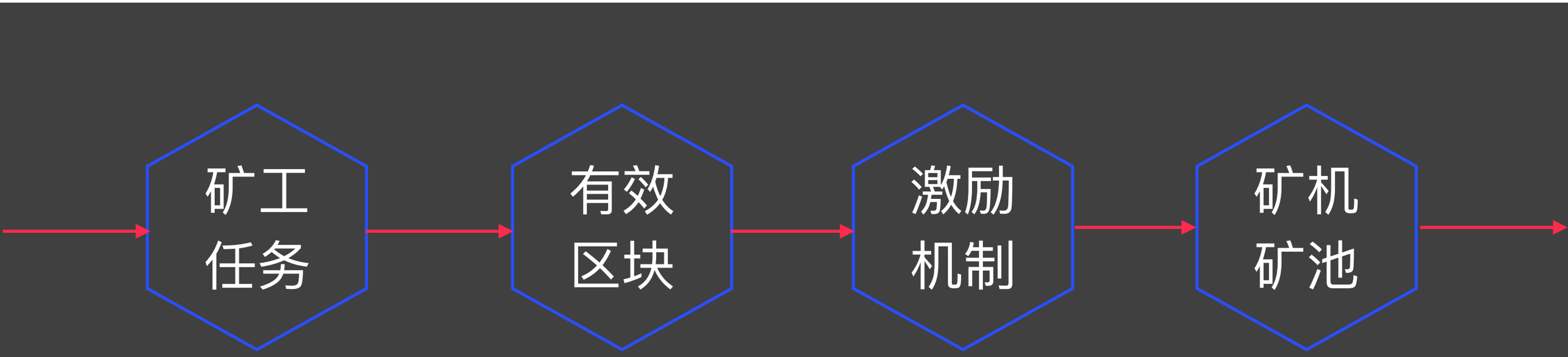

Node A
Node B
addr
getaddr
TIME
addr
addr
addr

协议


Node A
Node B
getblocks
getblocks
inv
getdata
block
block
block
block
block
block
TIME


Node A
Node B
getheaders
headers
getheaders
headers
TIME

挖矿

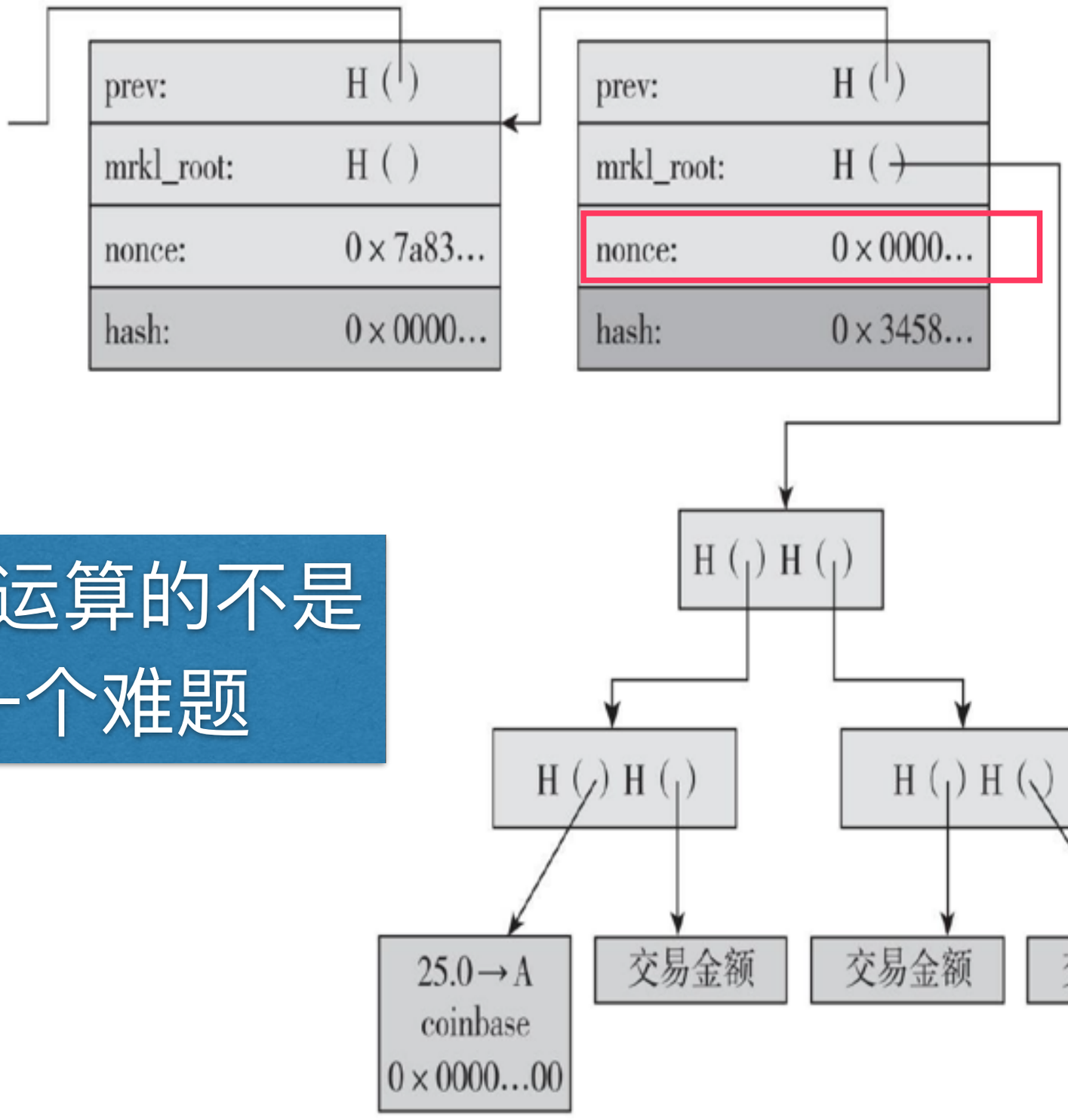


矿工的任务

- 监听交易广播
- 维护区块链网络和监听新的区块
- 组装一个备选区块
- 找到一个让你的区块有效的随机数
- 希望你的区块被全网接受
- 利润

验证交易和区块 vs. 和其余矿工竞争

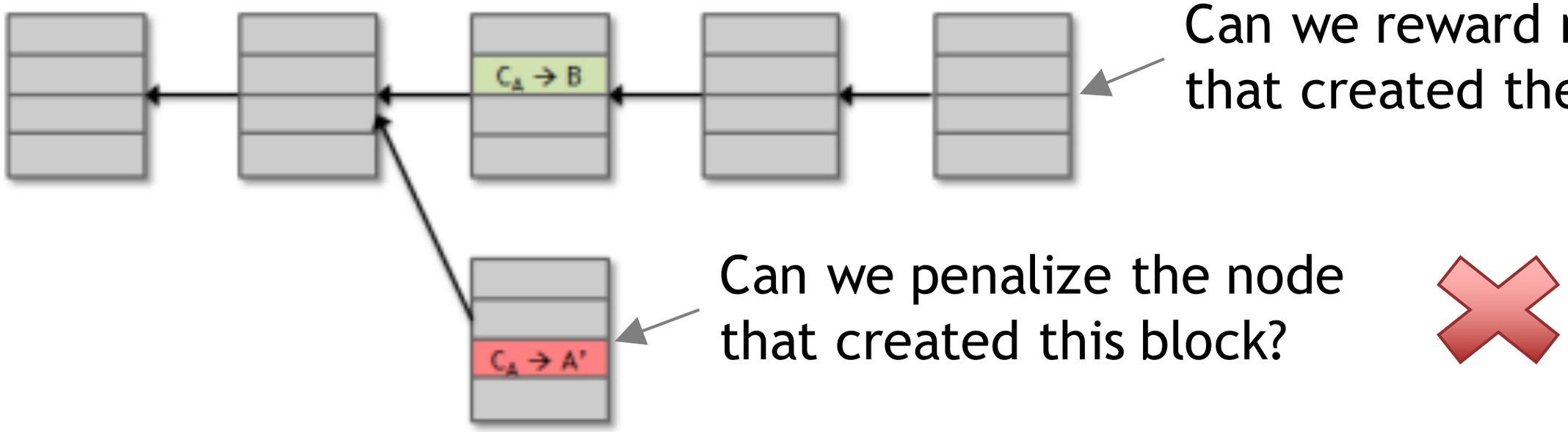
寻找有效区块



32位随机数

每个人运算的不是同一个难题

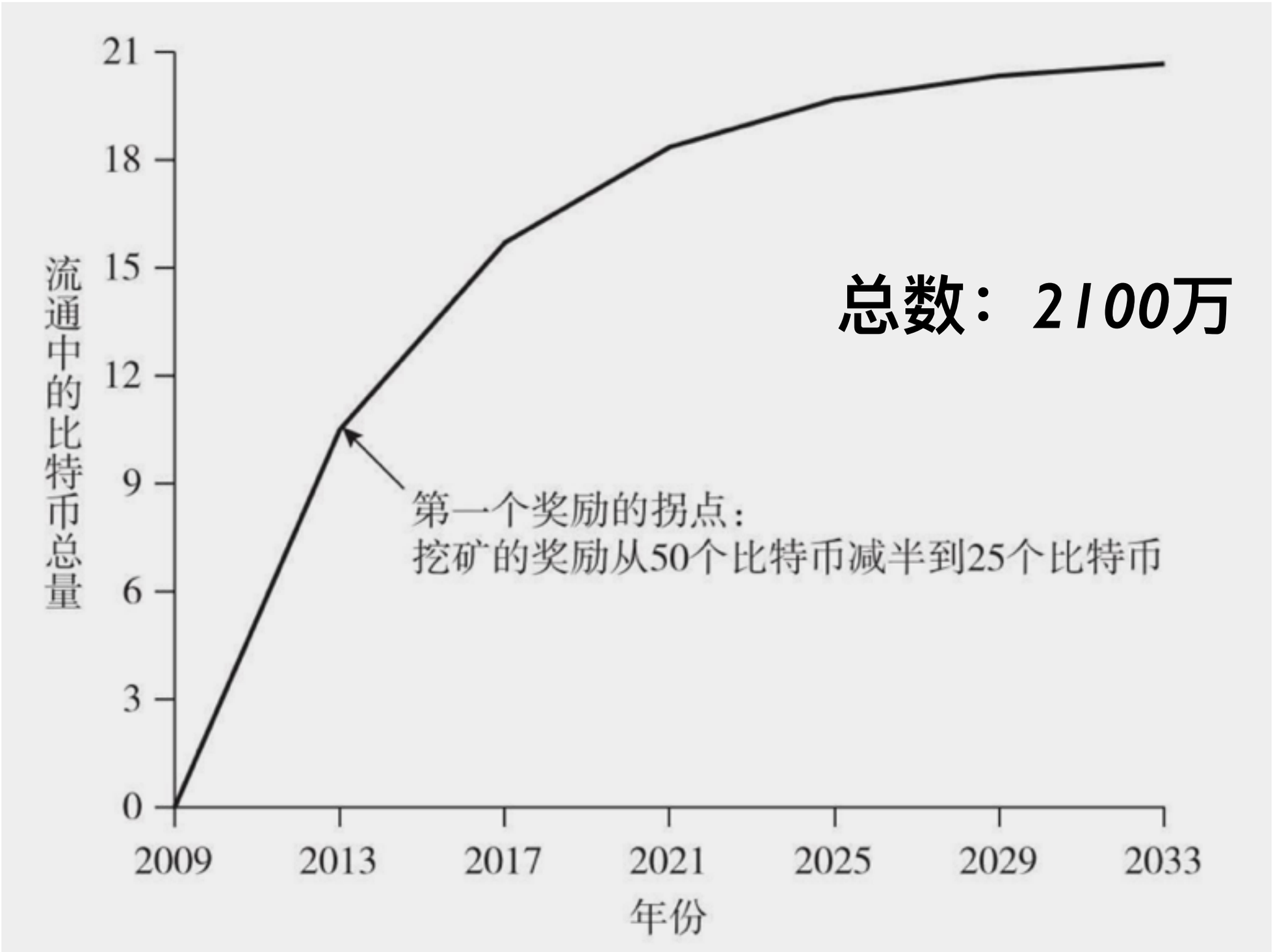
激励节点诚实



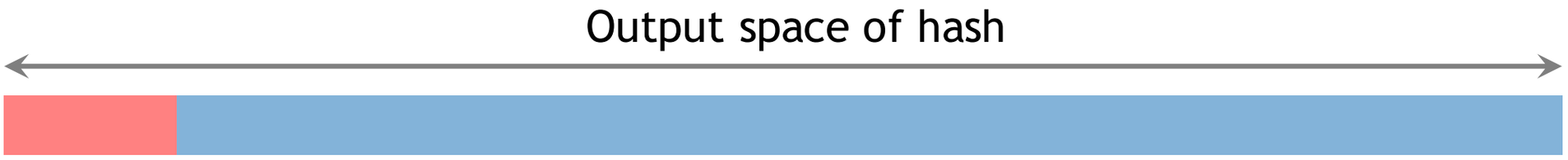
区块奖励 *vs.* 交易费奖励

交易费：输入和输出不等

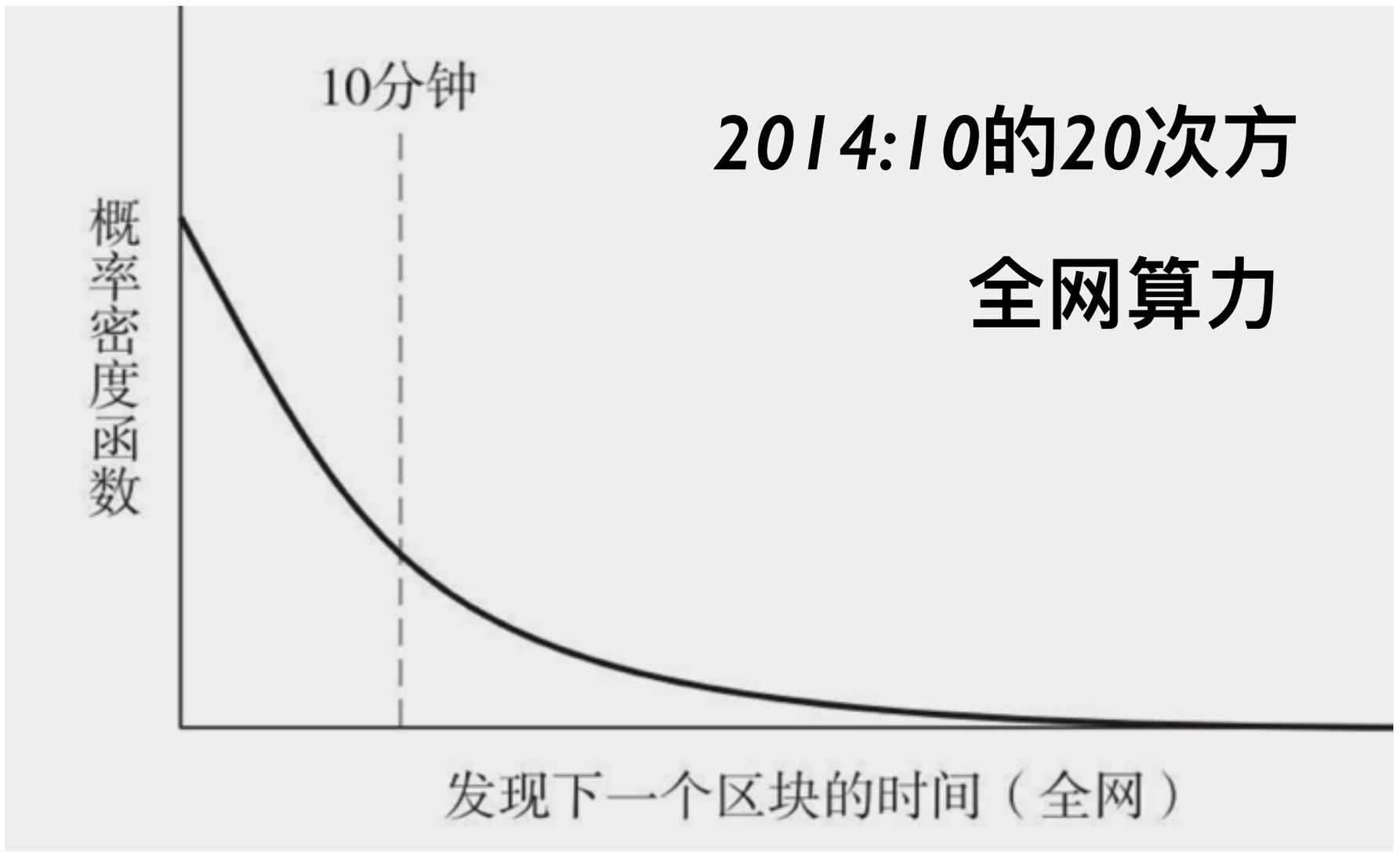
比特币奖励


流通中的比特币总量
21
18
15
12
9
6
3
0
2009
2013
2017
2021
2025
2029
2033
年份
总数：2100万
第一个奖励的拐点：
挖矿的奖励从50个比特币减半到25个比特币

工作量证明



$$H(nonce \parallel prev\_hash \parallel tx \parallel tx \parallel \cdots \parallel tx) < target$$



2014:10的20次方

全网算力

限定*Hash*的输出范围

临时随机数

***PoW*：工作量证明**

***PoS*：权益证明**

挖矿发展

CPU

GPU

FPGA

ASIC

gold pan

sluice box

placer mining

pit mining

专业矿场

温度

电费

网速

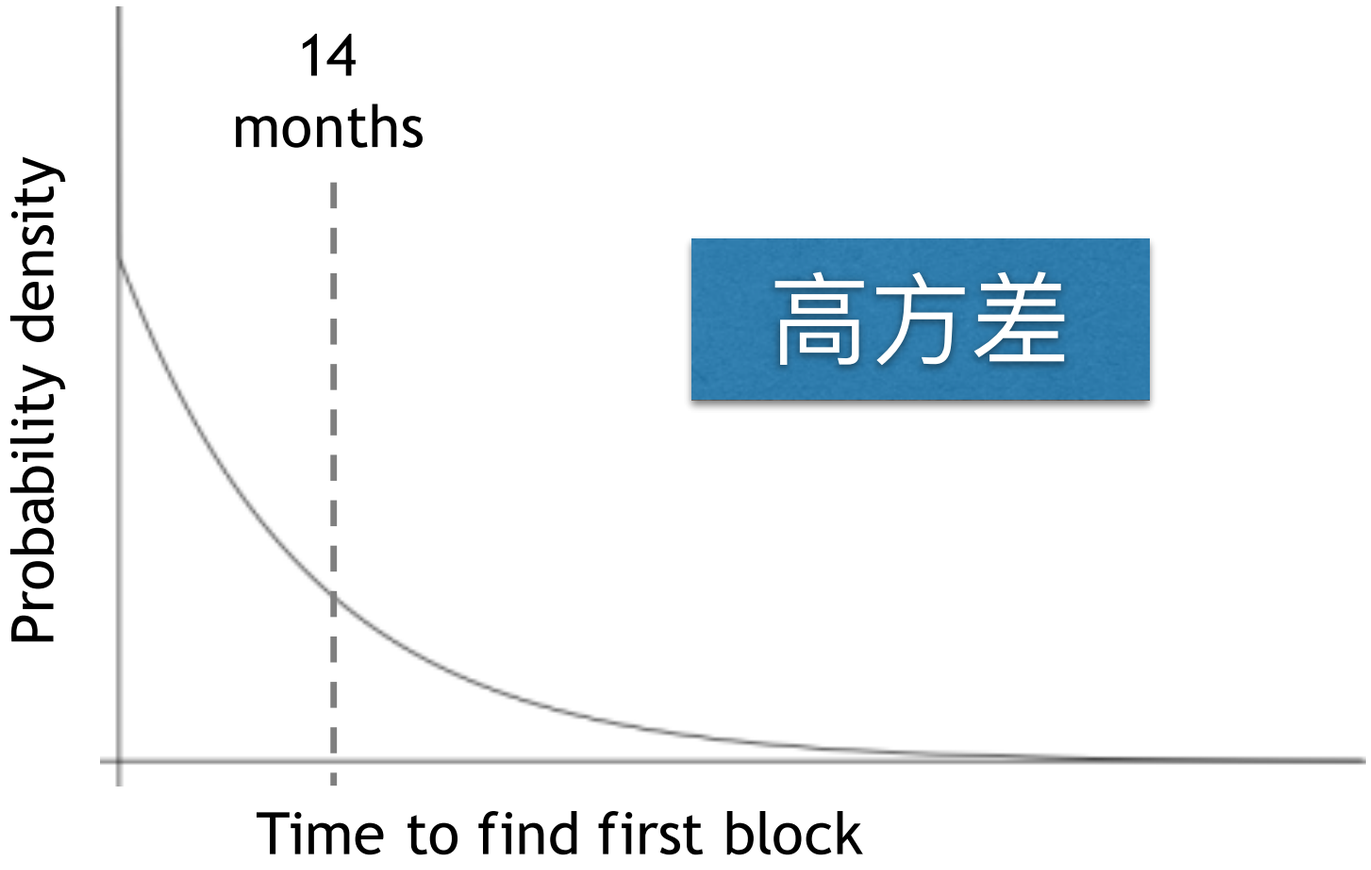
中国

矿池

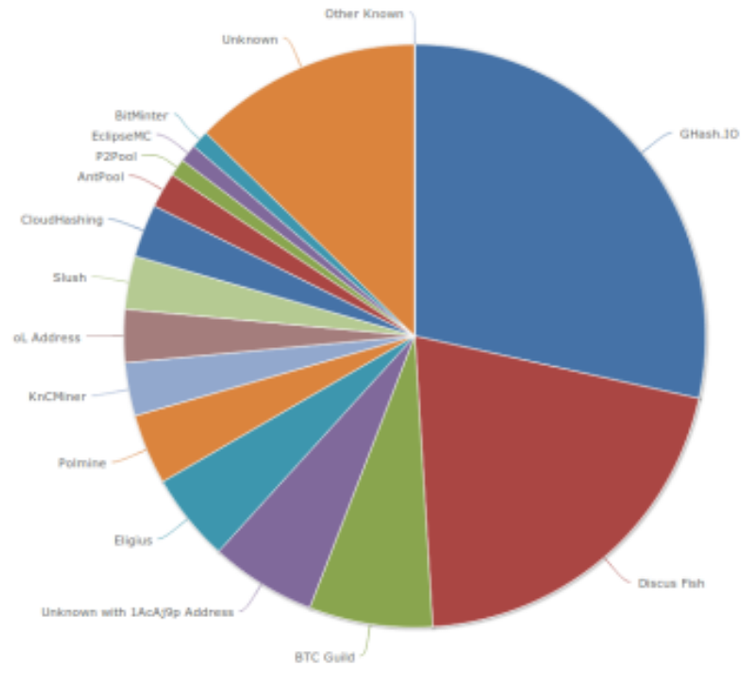
TerraMiner IV

Cost: ≈US$6,000
Expected time to find a block: ≈14 months
Expected revenue: ≈$1,000/month

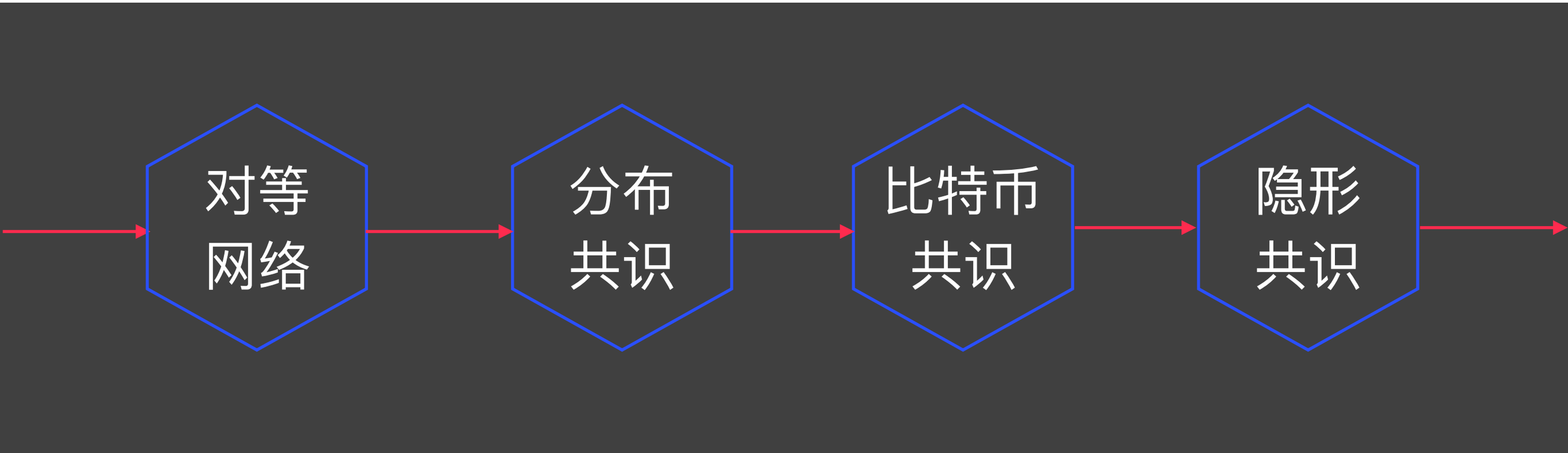
# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%



高方差



共识



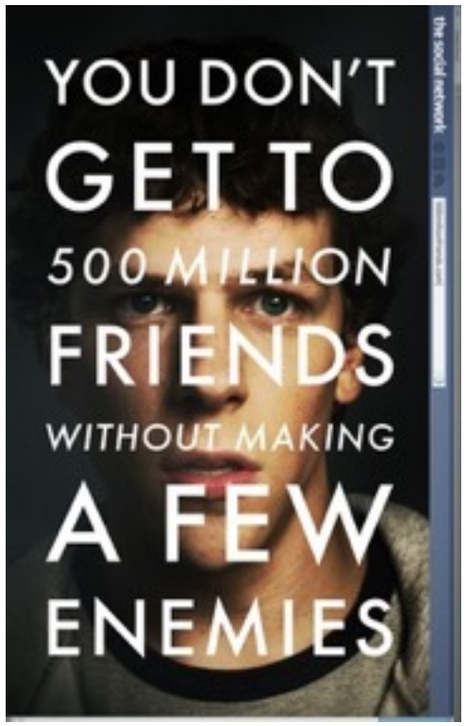
Peer to Peer

napster™

1999

Sean Parker

facebook

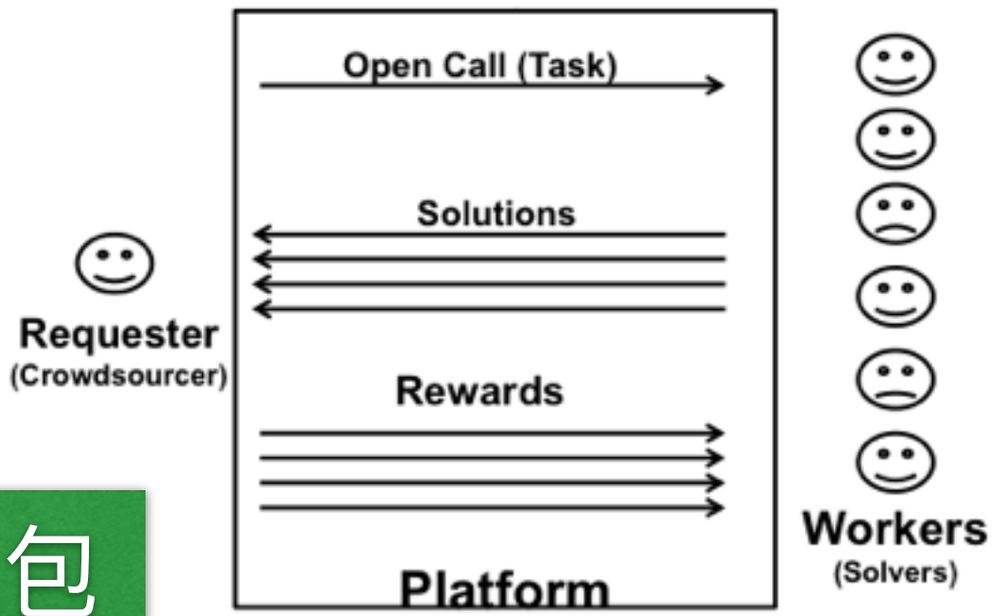


The Social Network

skype™

2003

KaZaA



众包

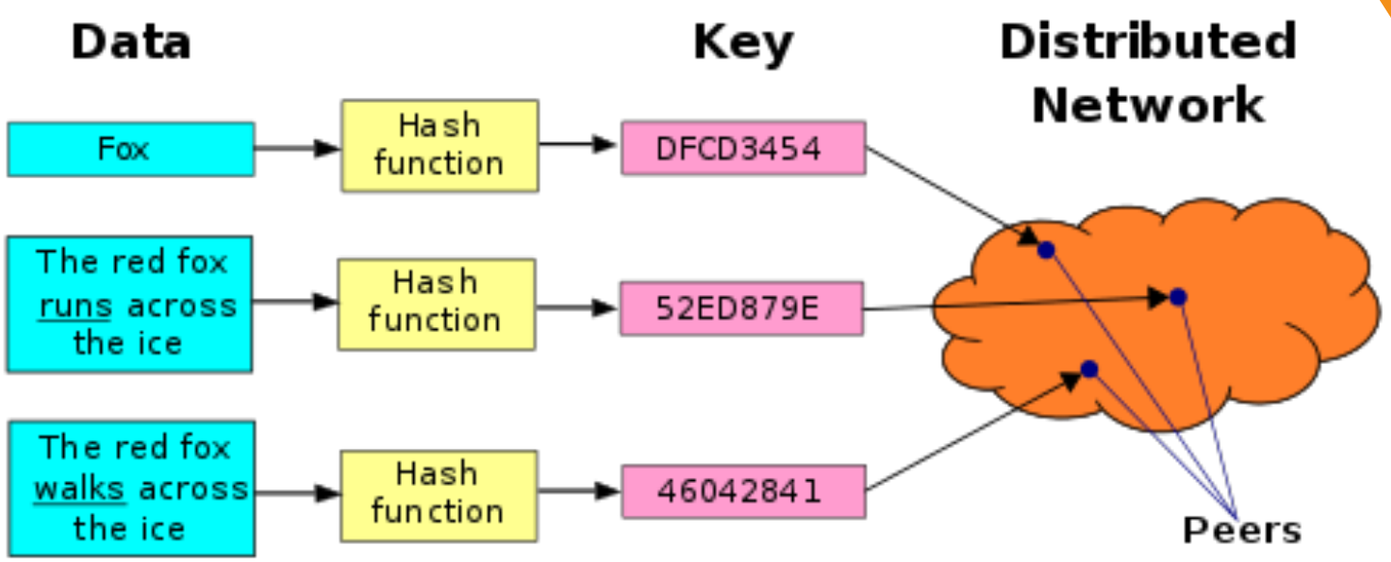
BitTorrent

2001

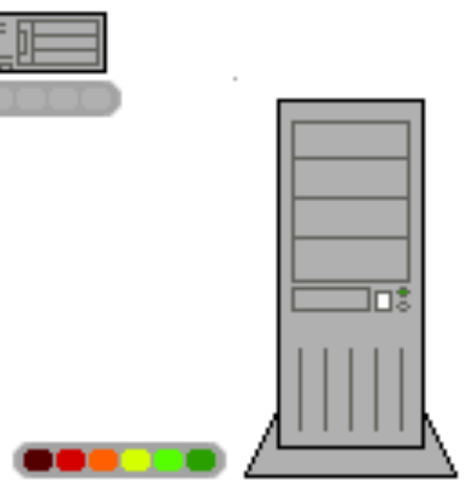
Bram Cohen

BitTorrent

Distributed Hash Table



https://en.wikipedia.org/wiki/Distributed_hash_table



激励

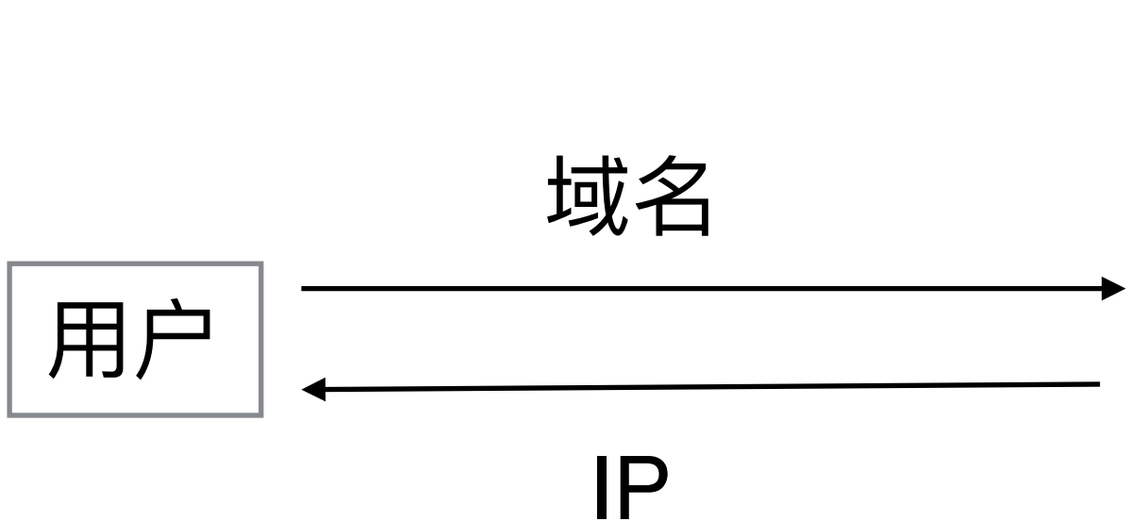
https://en.wikipedia.org/wiki/BitTorrent

分布共识

- 在一个有*n*个节点的系统中，每一个节点都有一个输入值，其中有一些节点是错误的或者恶意的。一个分布式共识协议具有如下两个属性：

  ✳ 结束时所有诚实的节点均认同该值；

  ✳ 该值由诚实节点产生



Distributed DB, Email, PKI

拜占庭将军问题和Paxos

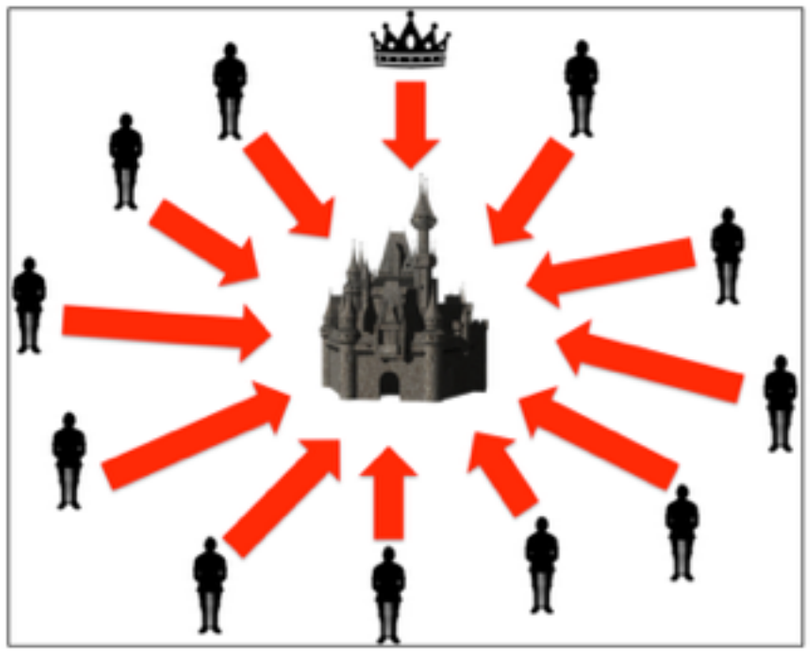
LESLIE LAMPORT

2013图灵奖

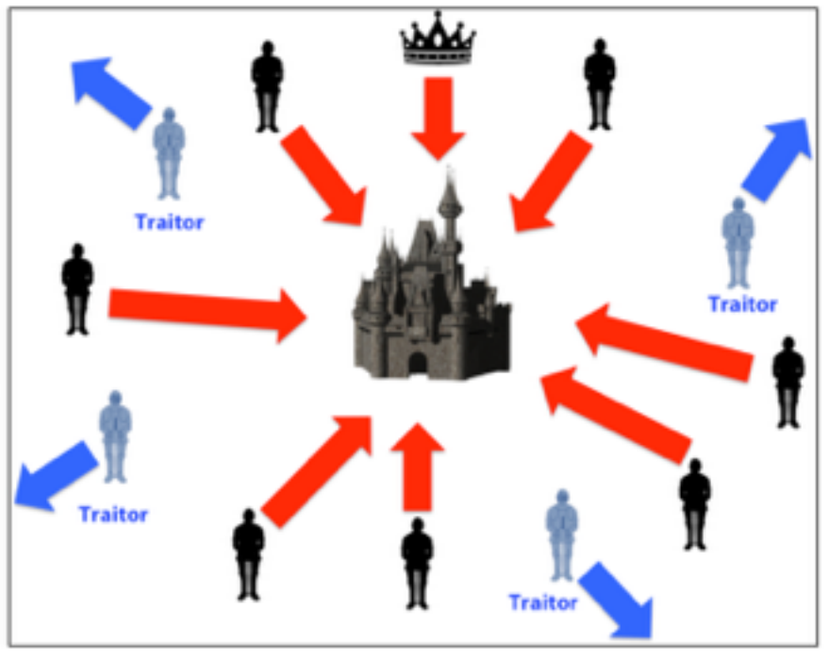
The Byzantine Generals Problem

1982

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International



Coordinated Attack Leading to Victory



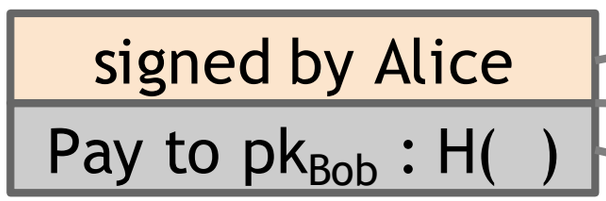
Uncoordinated Attack Leading to Defeat

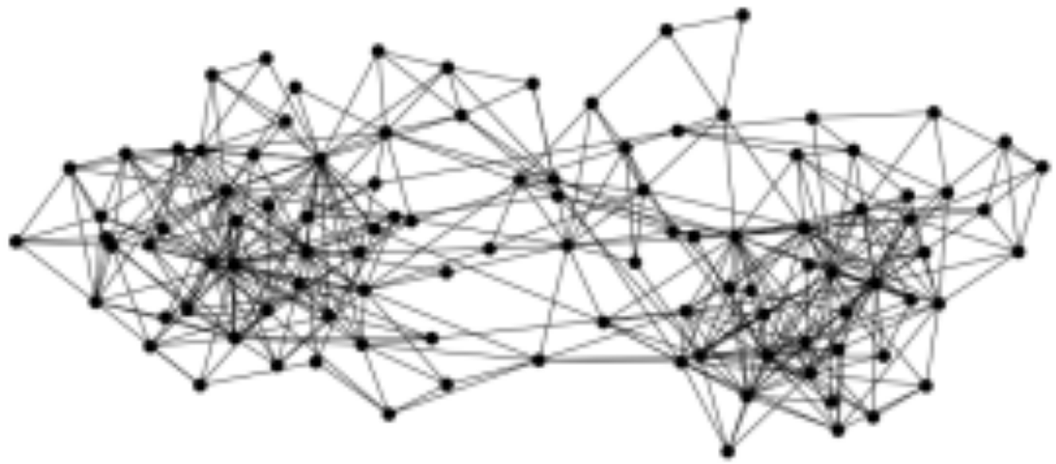
Paxos Made Simple

2001

The Paxos algorithm, when presented in plain English, is very simple.

比特币的交易传播

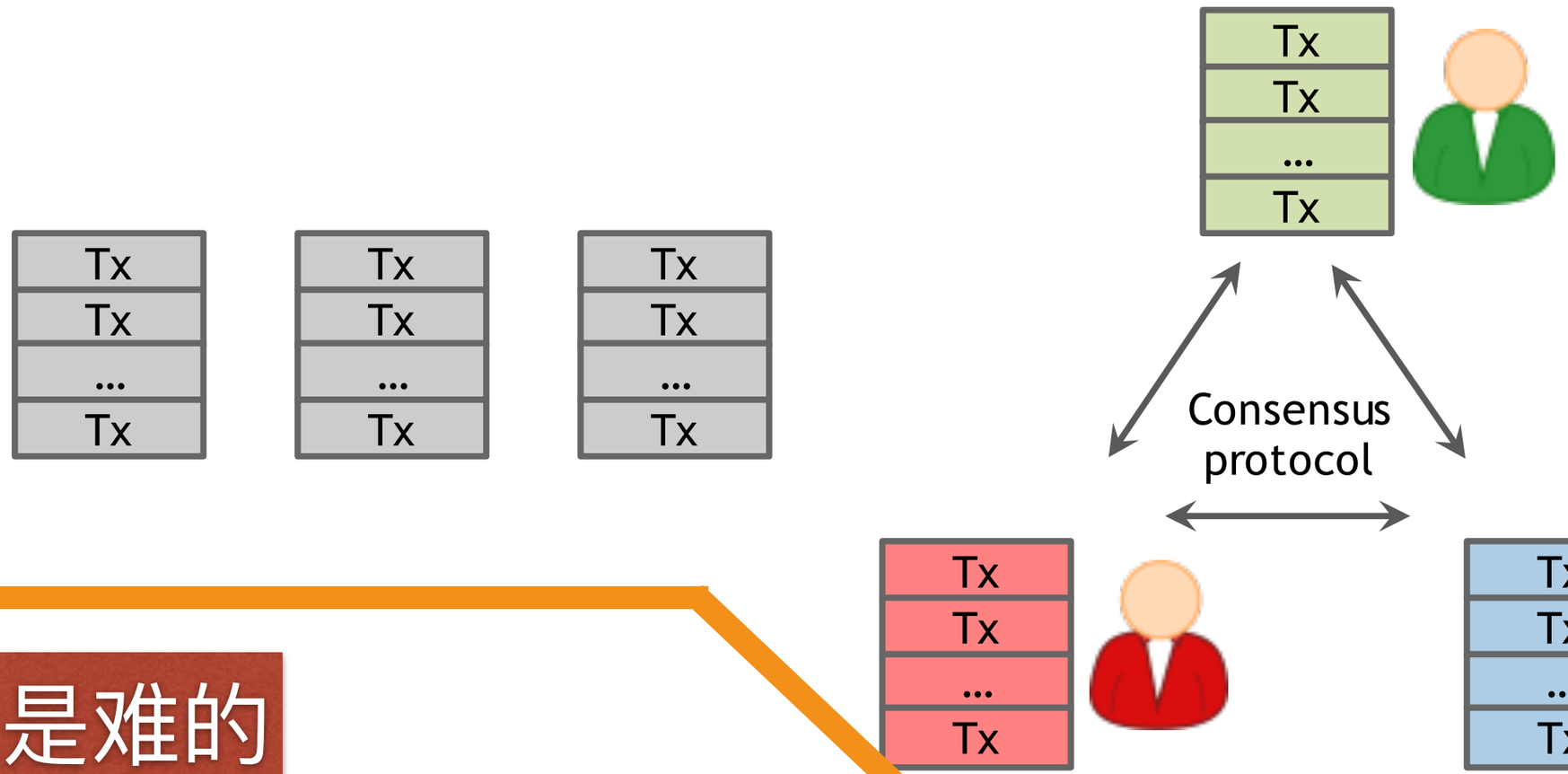




- 比特币是一个*P2P*网络
- *Alice* 需要广播她完成的交易給所有的节点
- *Bob*计算机当时可以不在*P2P*网络中
- *A single, global ledger for the system*
- 等待共识的业务、已共识的业务

比特币的分布共识

每一个节点输出它的未共识的业务竞争下一个Block



共识是难的

➡ *Node: crash, malicious*

➡ *Network: Imperfect (online, latency)* → *Global Time*

比特币和身份

- 比特币节点需要身份 *(ID)*
- 比特币假设恶意节点小于*50%*
- 但是*P2P*系统中，*ID*面临很大问题
  - ✴ *Sybil Attack*
- *Pseudonymity*是比特币的目的

- 比特币跟踪和验证*ID*是困难的
- 比特币采用的应对方法：随机的选择节点

比特币的隐形共识机制

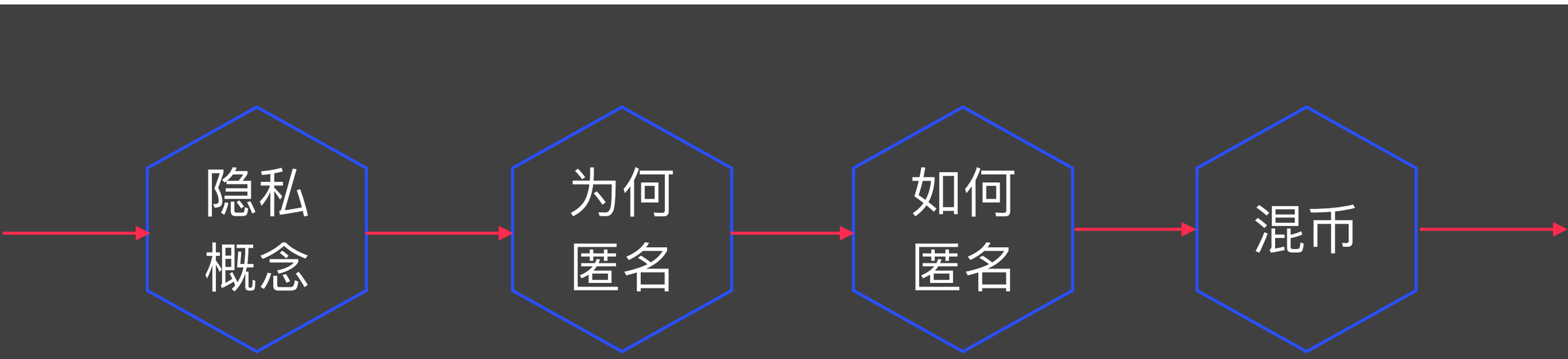
- 新的交易被广播到所有节点
- 每个节点将新的交易放进一个区块
- 在每一轮中，一个随机的节点被选择可以广播它的区块
- 其余节点可以选择接受这个区块，前提是区块的交易是可验证的
- 节点将以上区块的*Hash*放进自己的区块，表示它认可这个新区块

隐形共识：接受该块并扩展 vs. 拒绝该块，扩展前面的块

比特币的共识总结

- 理论落后于实践
- 引入了*Incentive*
  - ✳ 是电子货币
- 利用了随机性
  - ✳ 很长时间后才取得共识，*1*小时
  - ✳ 随着时间的增加，对某一块的共识的概率越来越大

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

公共空间

家庭

城邦

private: 私

privare: 剥夺

私人空间

社交空间

公共空间

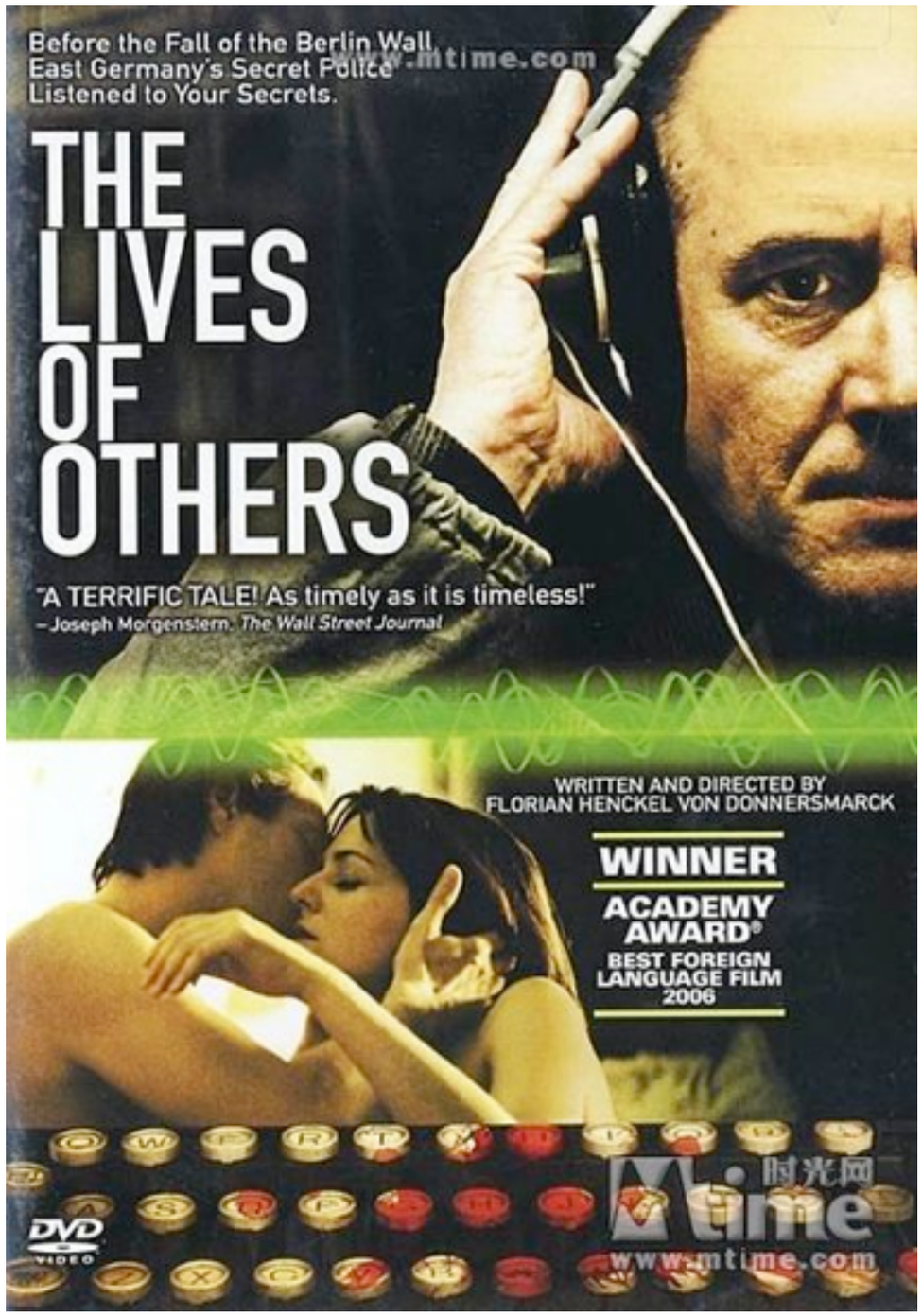
照相机　　摄像机　　网络

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

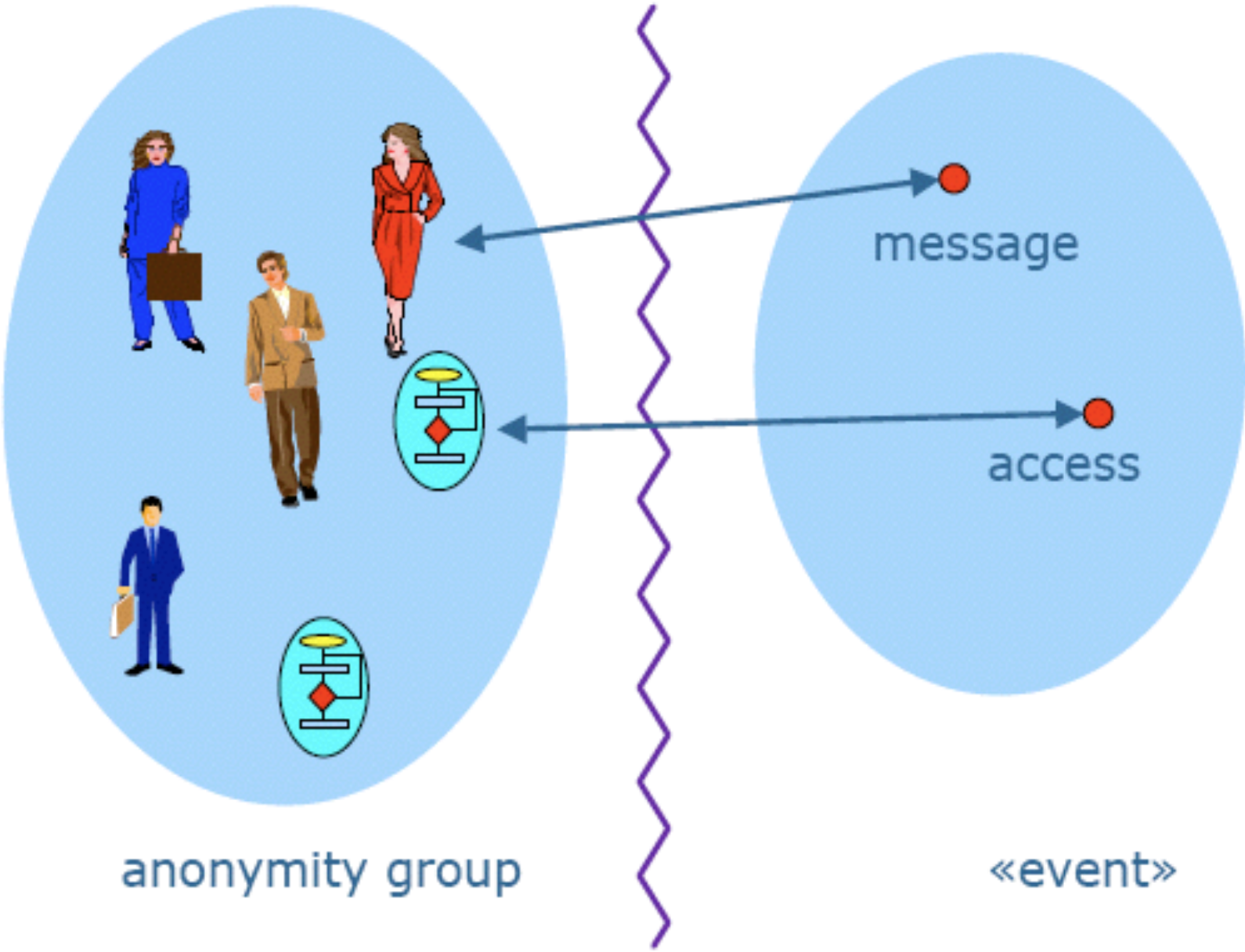
http://maherarar.net/

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

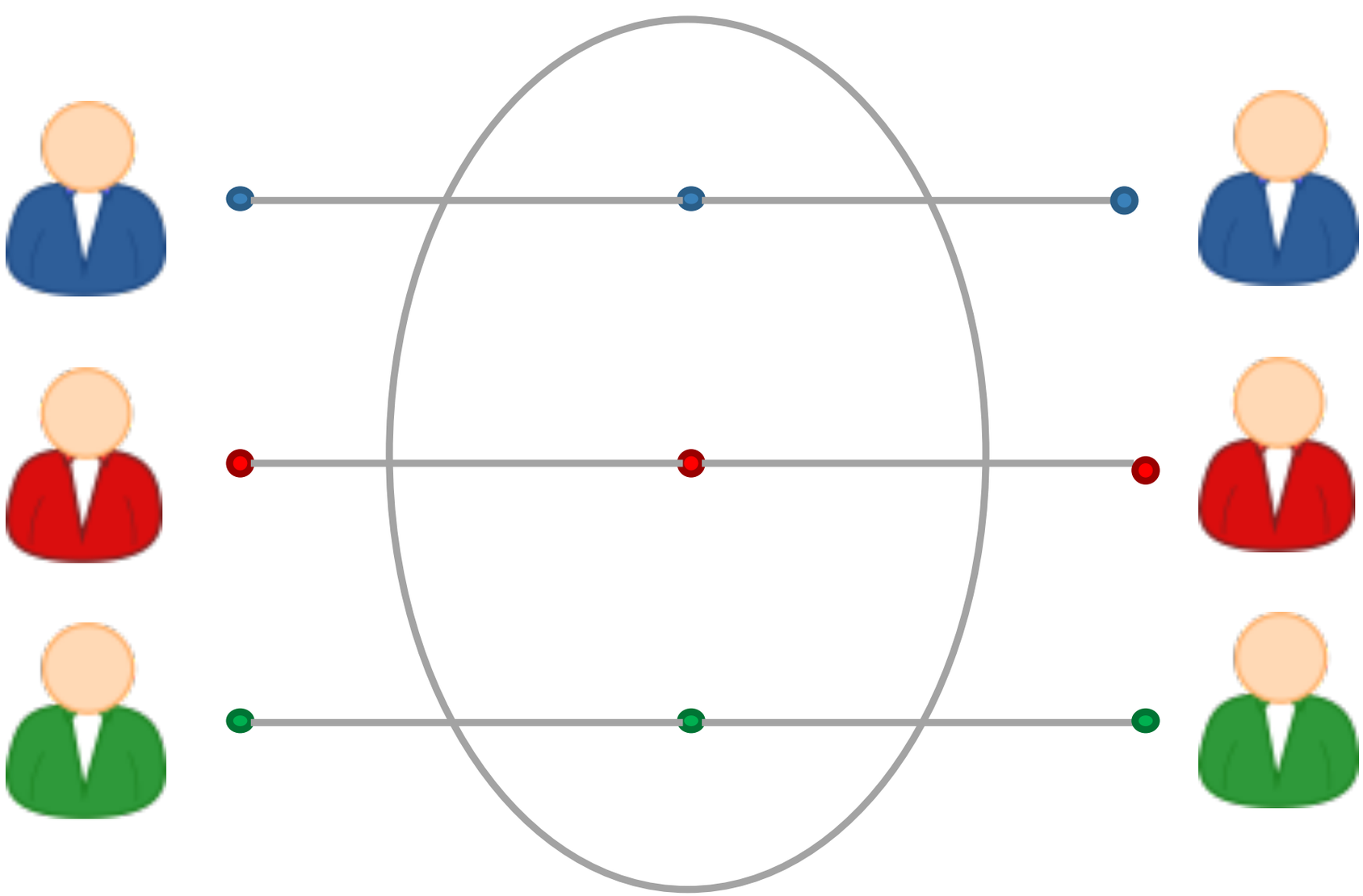
Name	Age	Gender	State of domicile	Religion	Disease
Ramsha	29	Female	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	Kerala	Hindu	Viral infection
Salima	28	Female	Tamil Nadu	Muslim	TB
sunny	27	Male	Karnataka	Parsi	No illness
Joan	24	Female	Kerala	Christian	Heart-related
Bahuksana	23	Male			
Rambha	19	Male			
Kishor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

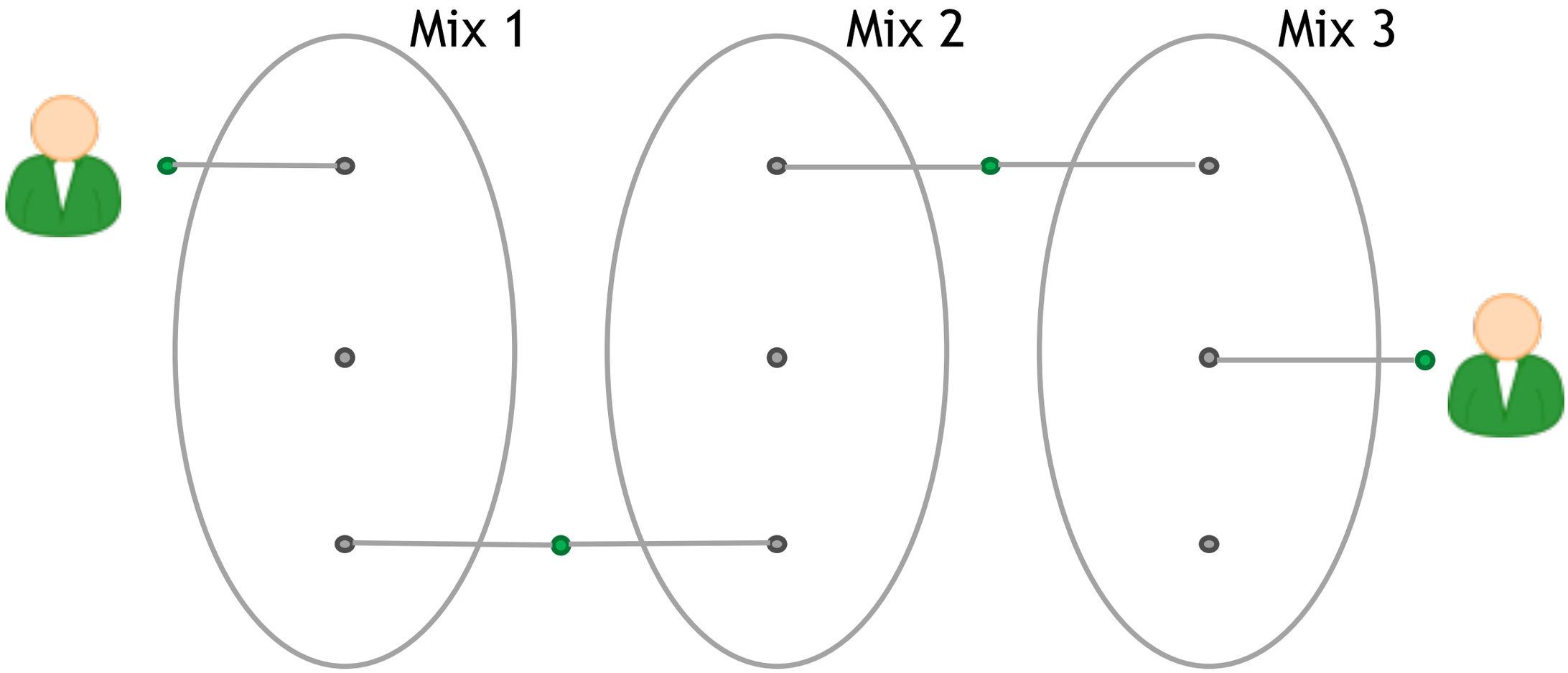


在线钱包

引入中介节点

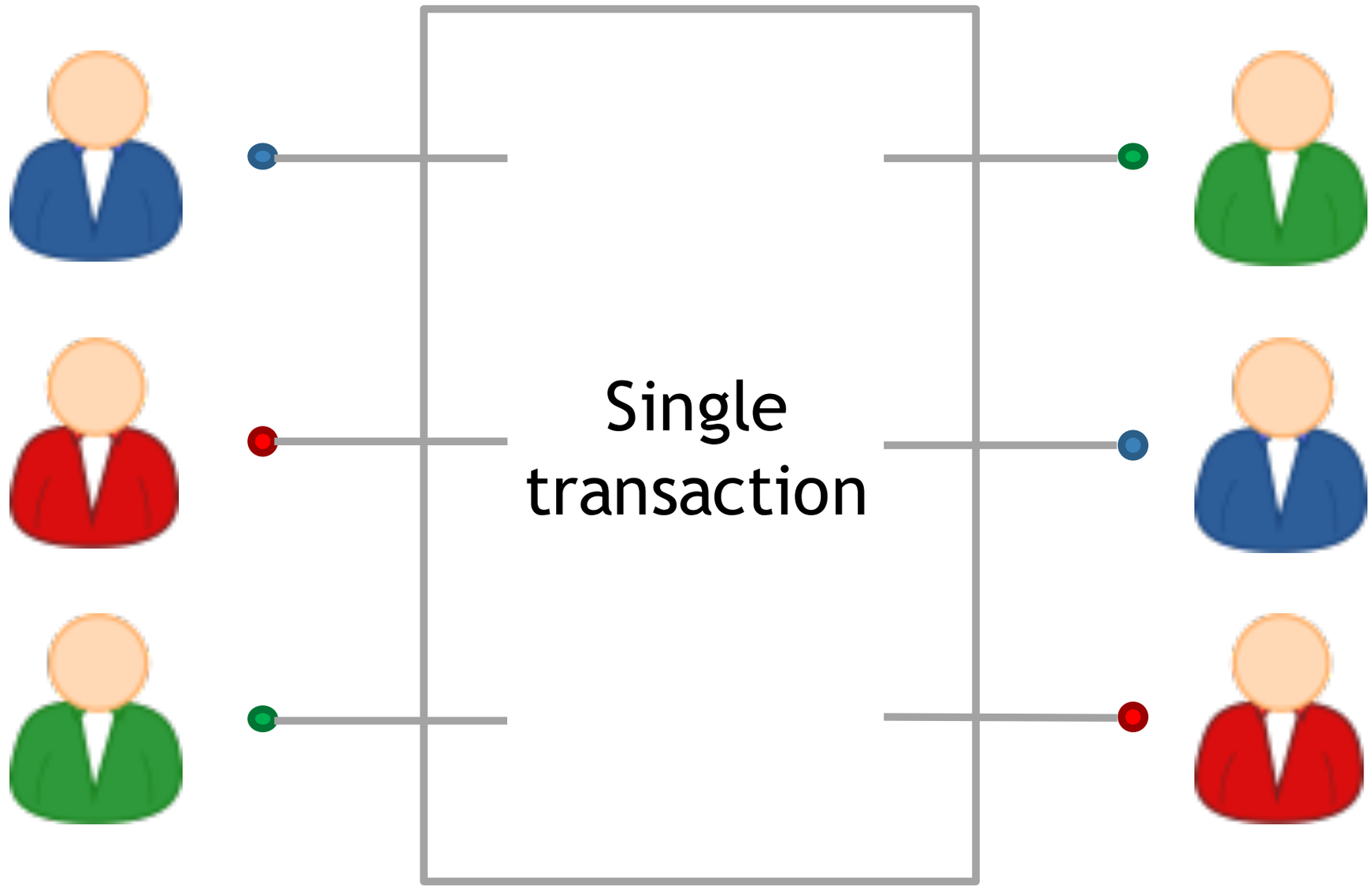
专项服务

多层混币



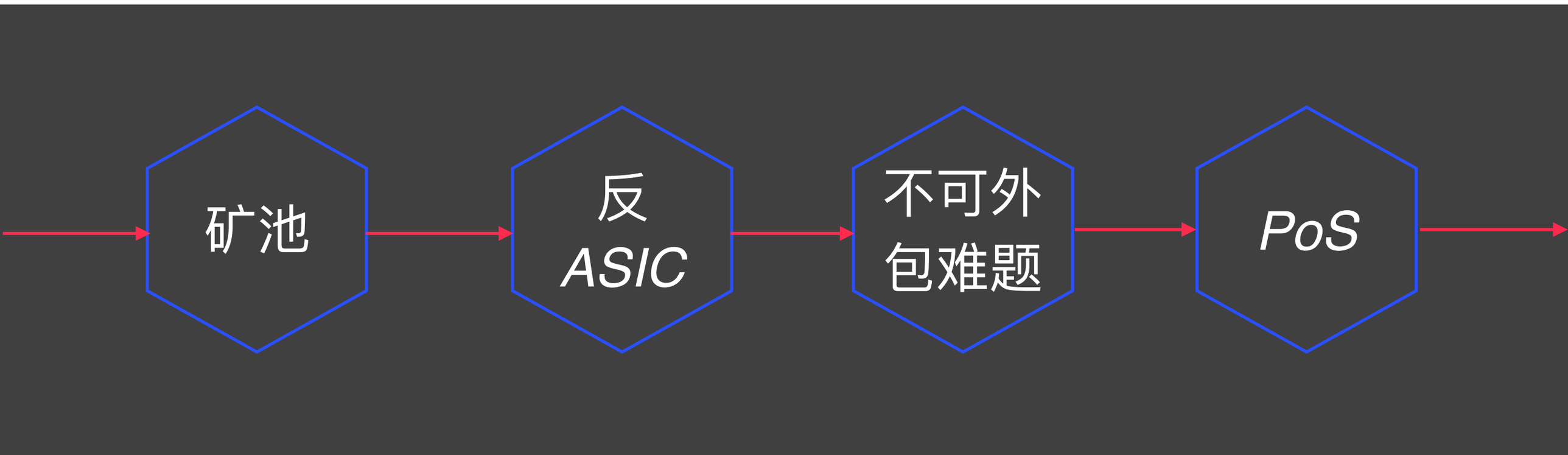
多重

分布式混币



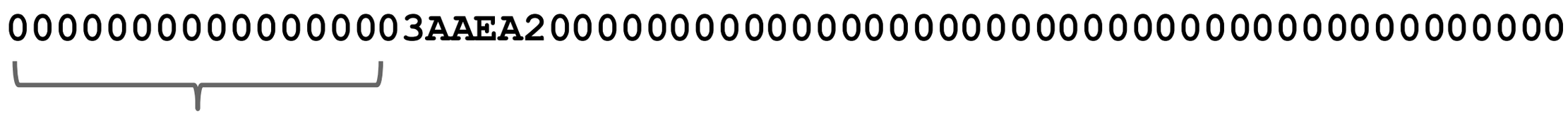
分布式

挖矿扩展



挖矿难度

256 bit hash output



当前难度 = $2^{66.2}$

下一个难度 = 上一个难度 * 2016 * 10分钟 / 产生上2016个区块所花费时间

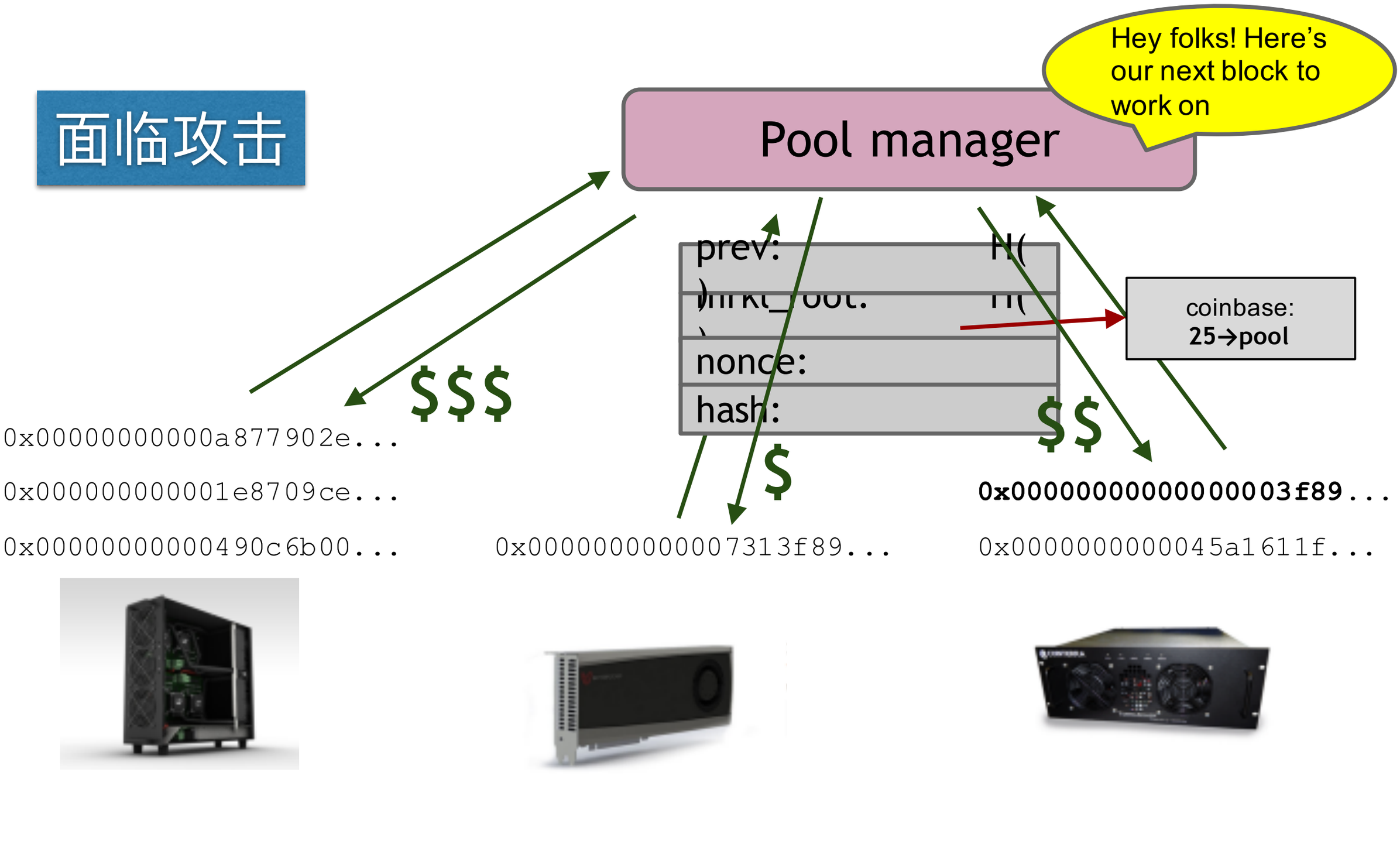
挖矿互助

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

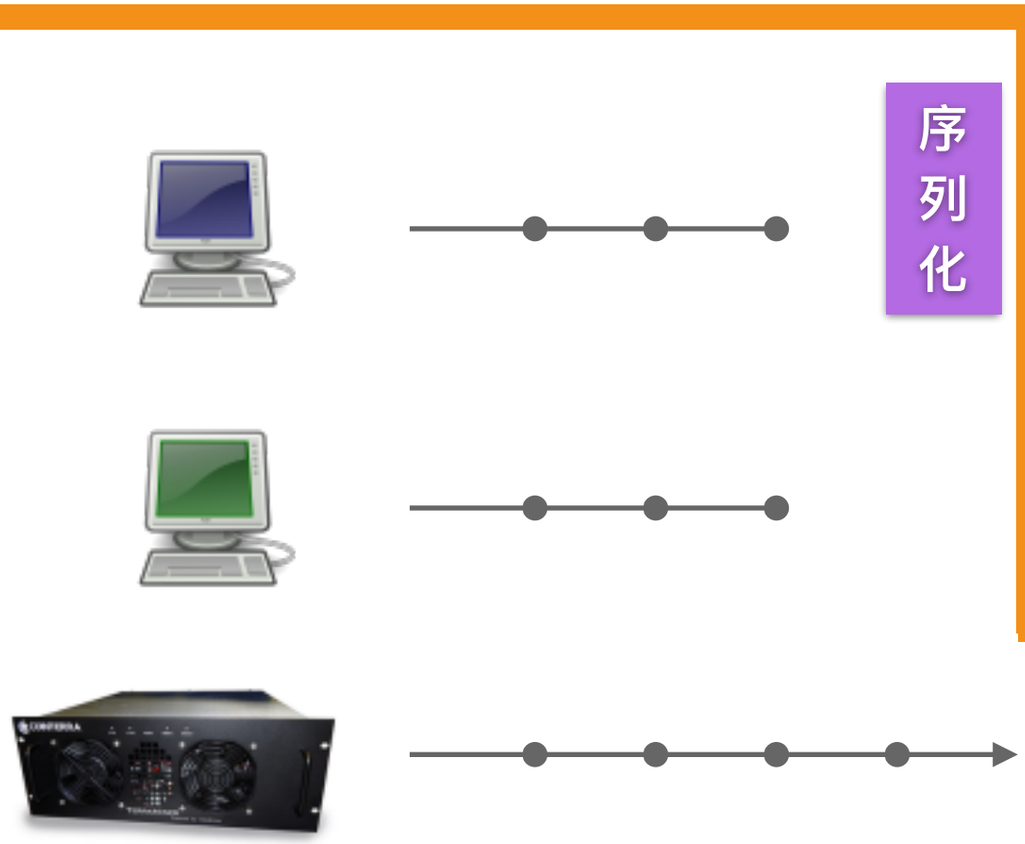

Hey folks! Here's our next block to work on
Pool manager
prev:
H(
)
nonce:
hash:
coinbase:
25→pool
$$$
$
$$
0x00000000000a877902e...
0x000000000001e8709ce...
0x0000000000490c6b00...
0x0000000000007313f89...
0x0000000000000003f89...
0x0000000000045a1611f...

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

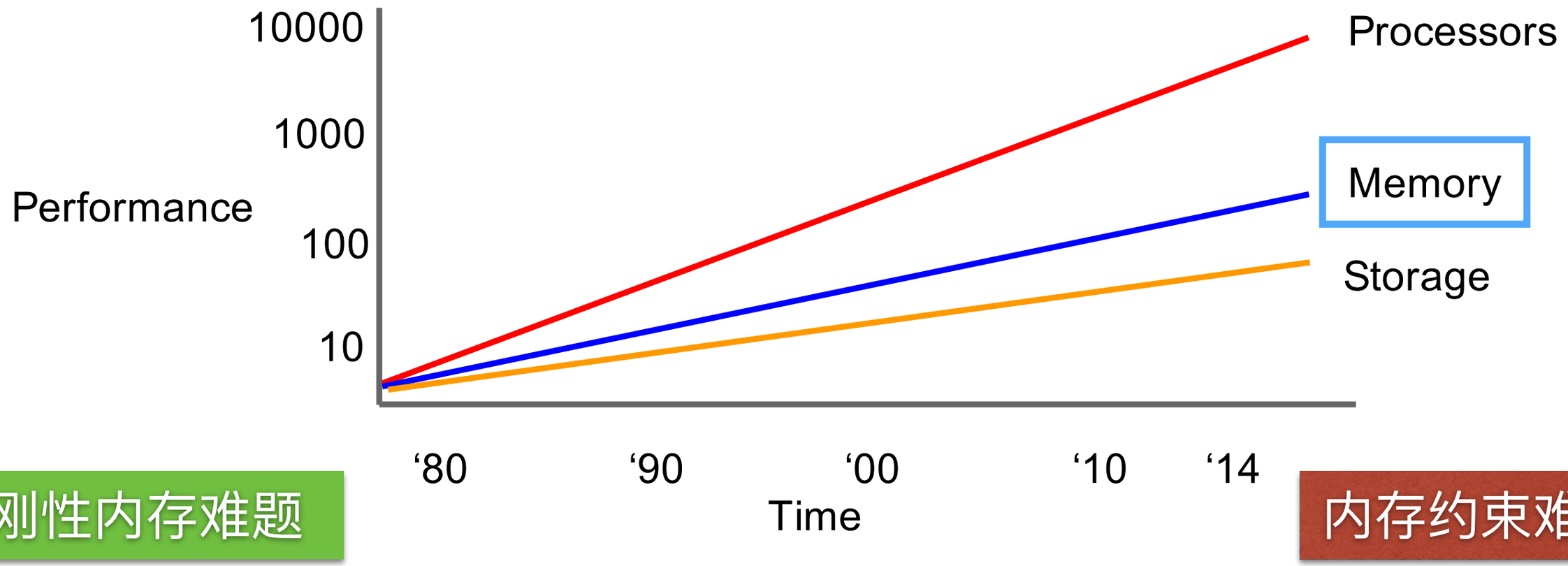
- 挖矿难题的结果要求验证简单
- 挖矿难题的难度可调节的特性
- 成功概率和所贡献的算力成比例



反ASIC







刚性内存难题

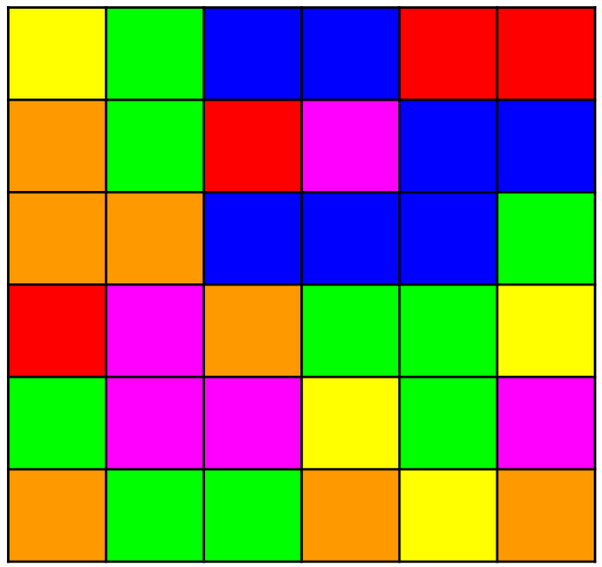
内存约束难题

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

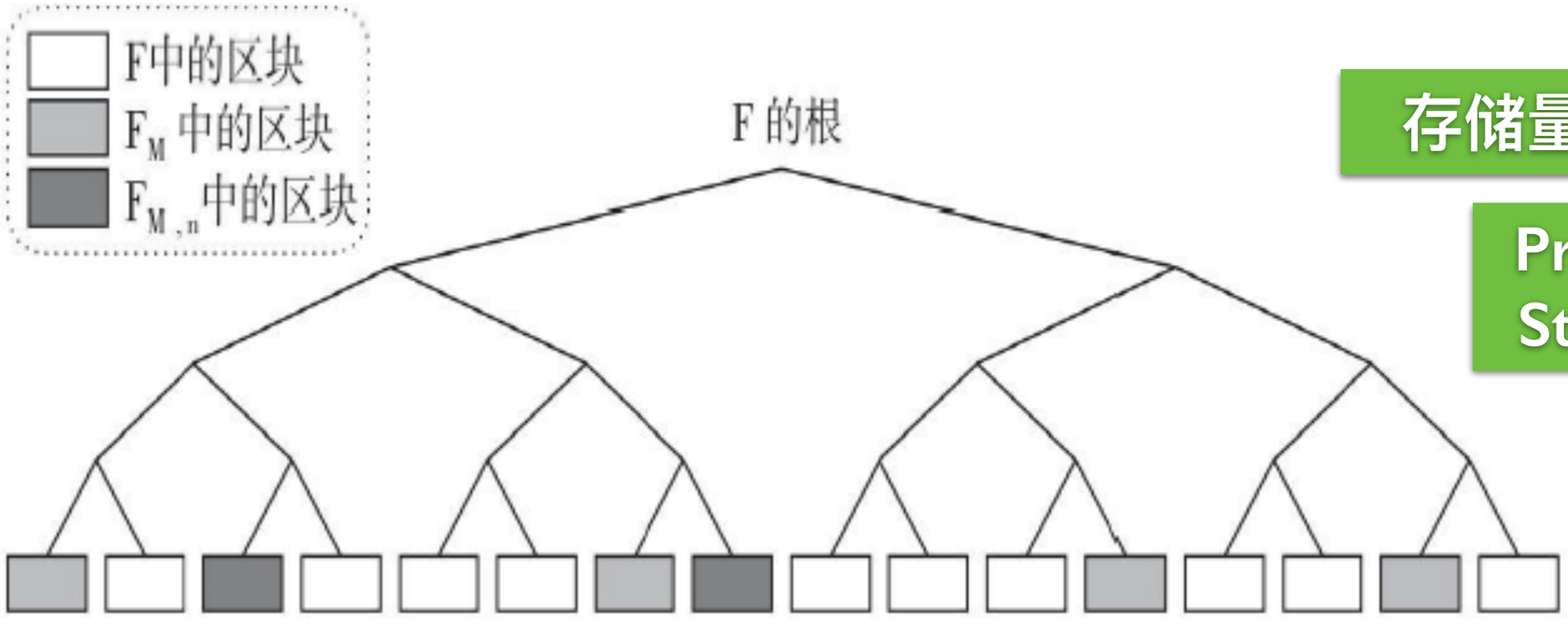
反ASIC是否有问题

有效工作量证明

挖矿能量消耗问题

志愿者计算项目

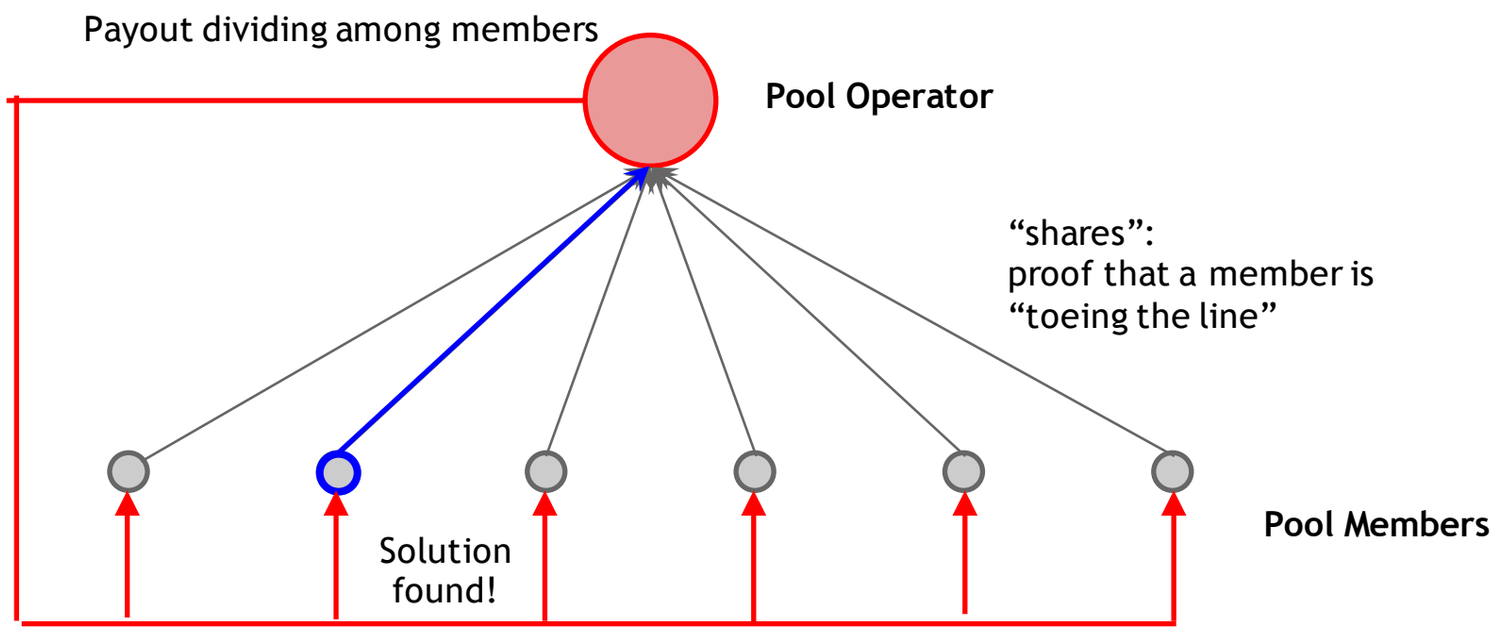
分布式存储



存储量证明

Proof of Storage

不可外包的难题



防止矿池的产生

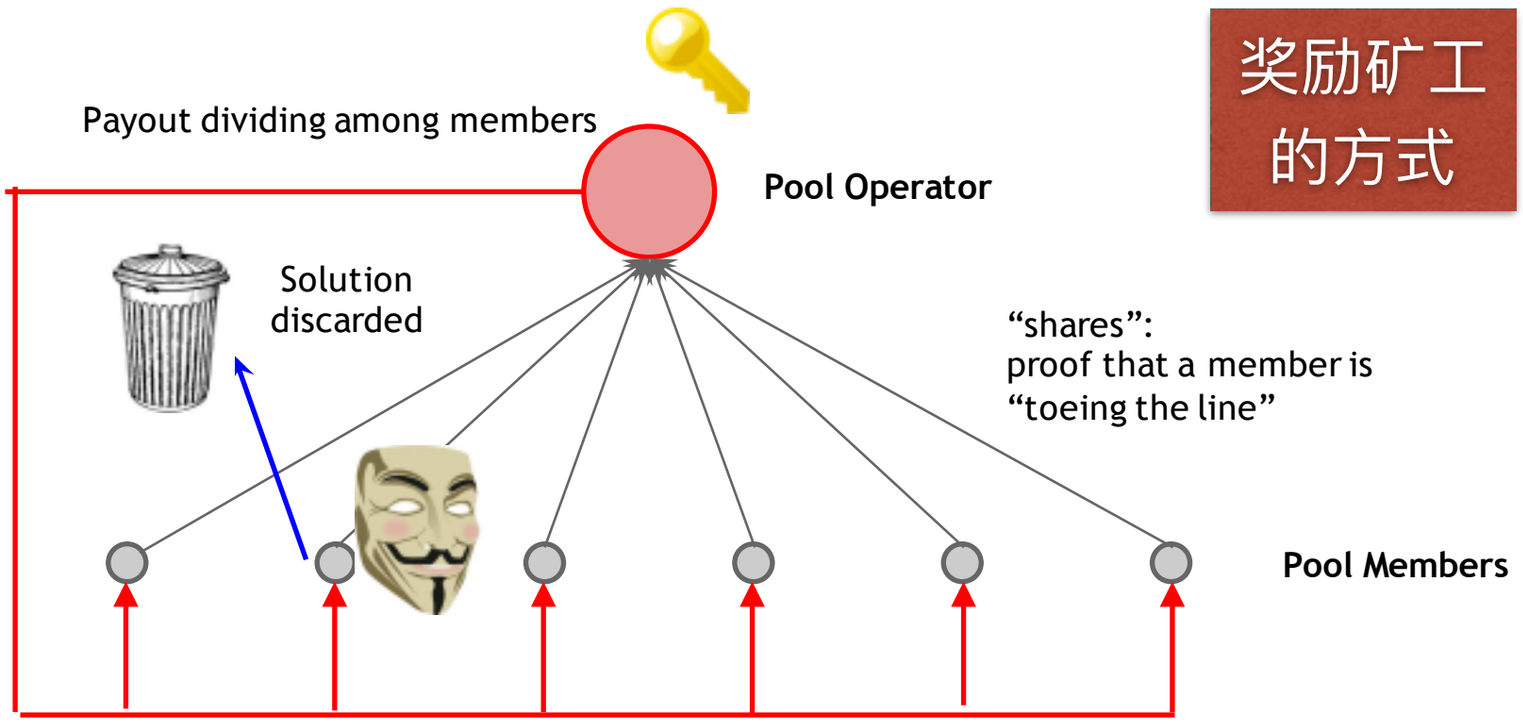
中心化、安全

区块丢弃攻击

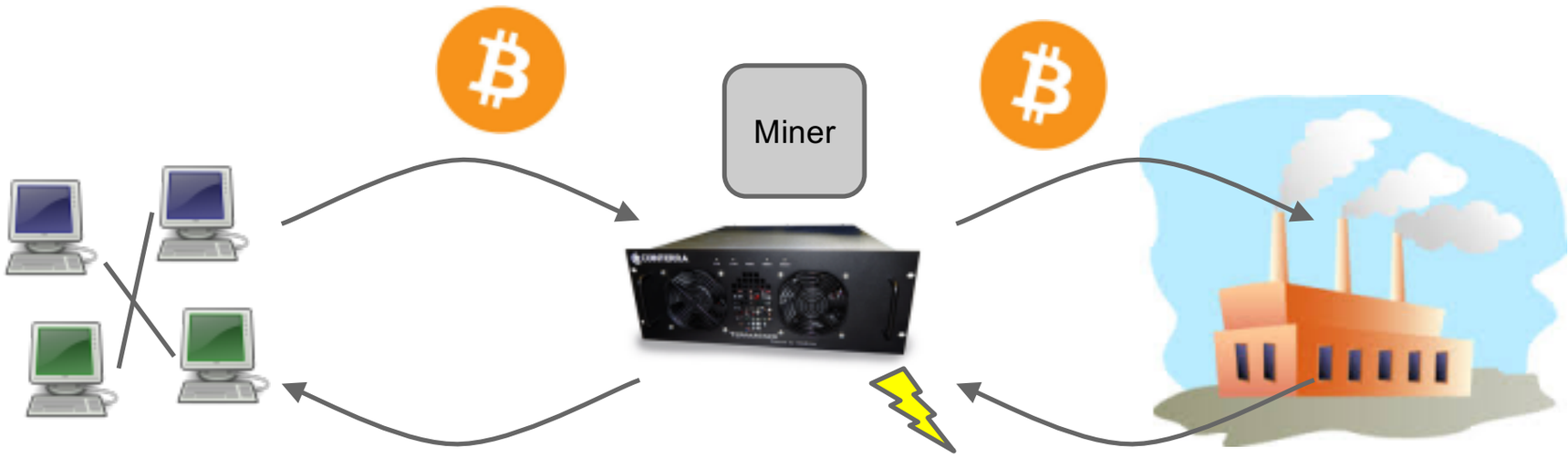
奖励破坏

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



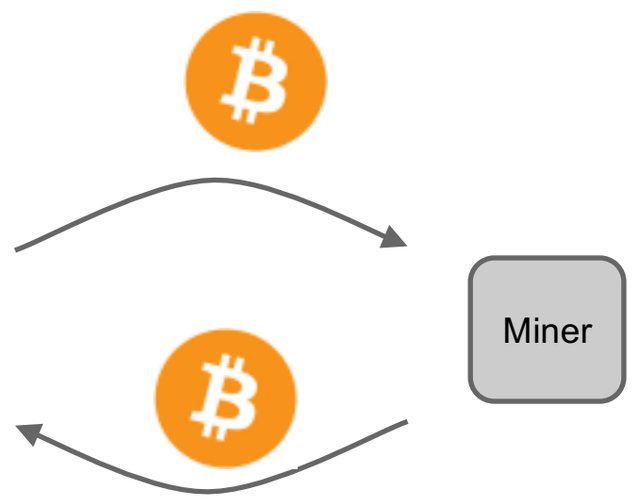
虚拟挖矿



权益证明

分叉攻击

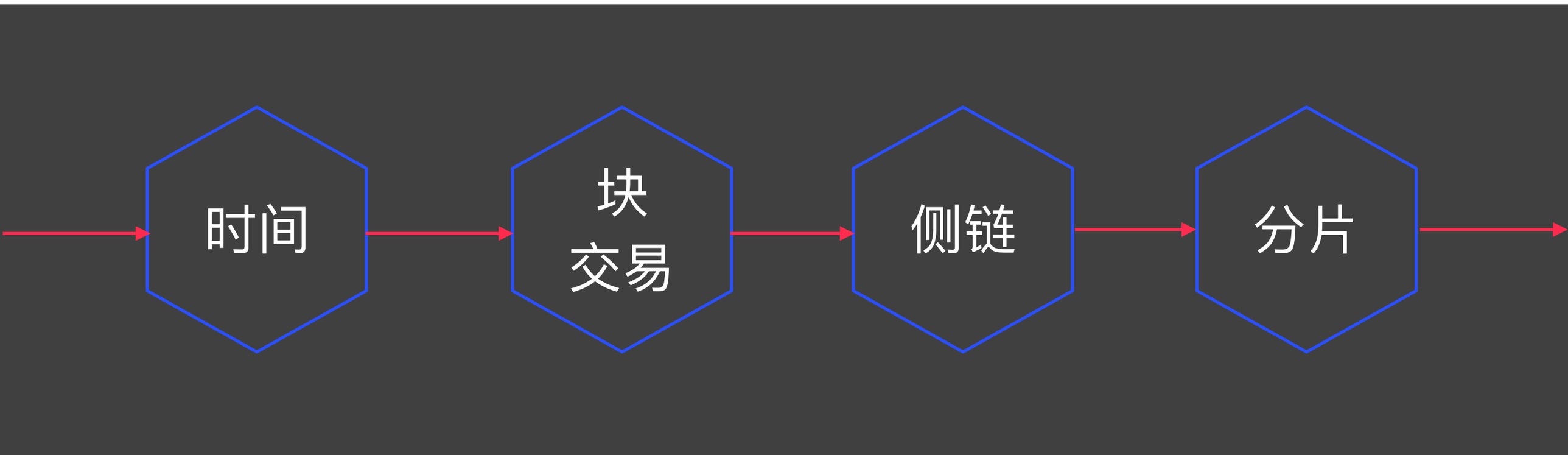
检查点



2012 点点币

币拥有量交易

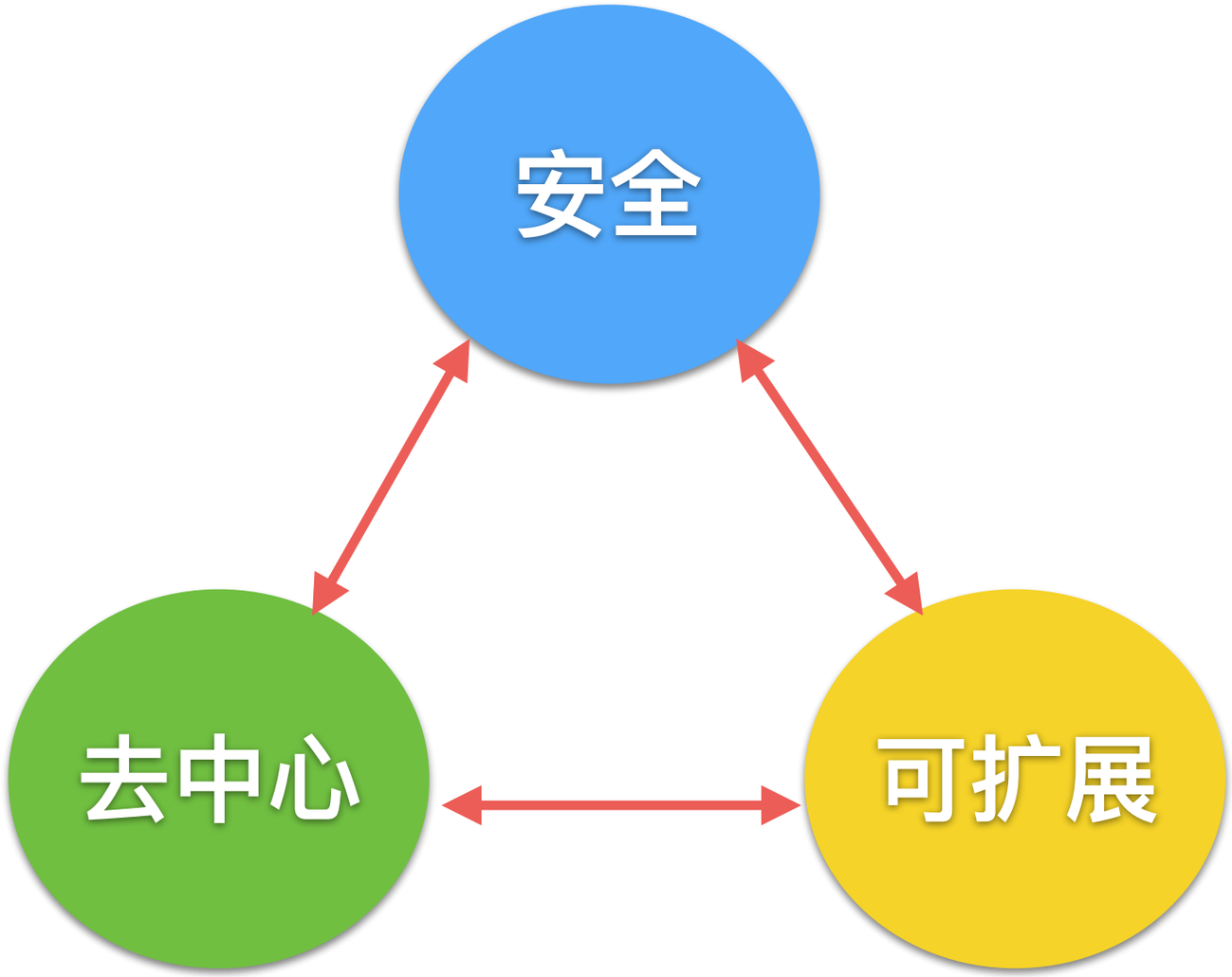
性能扩展



区块链可扩展性

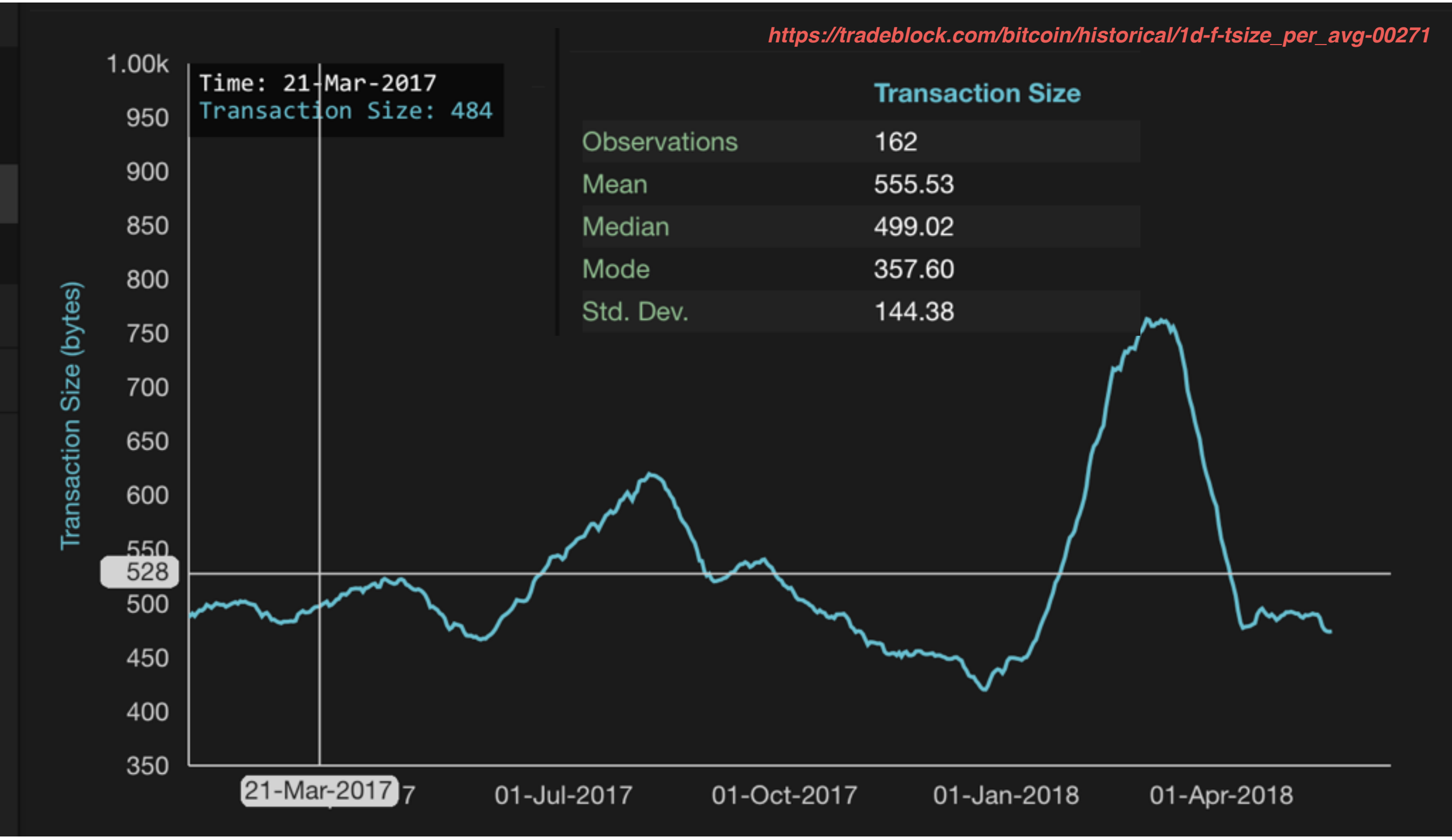
交易容量

产生块时间



比特币的TPS

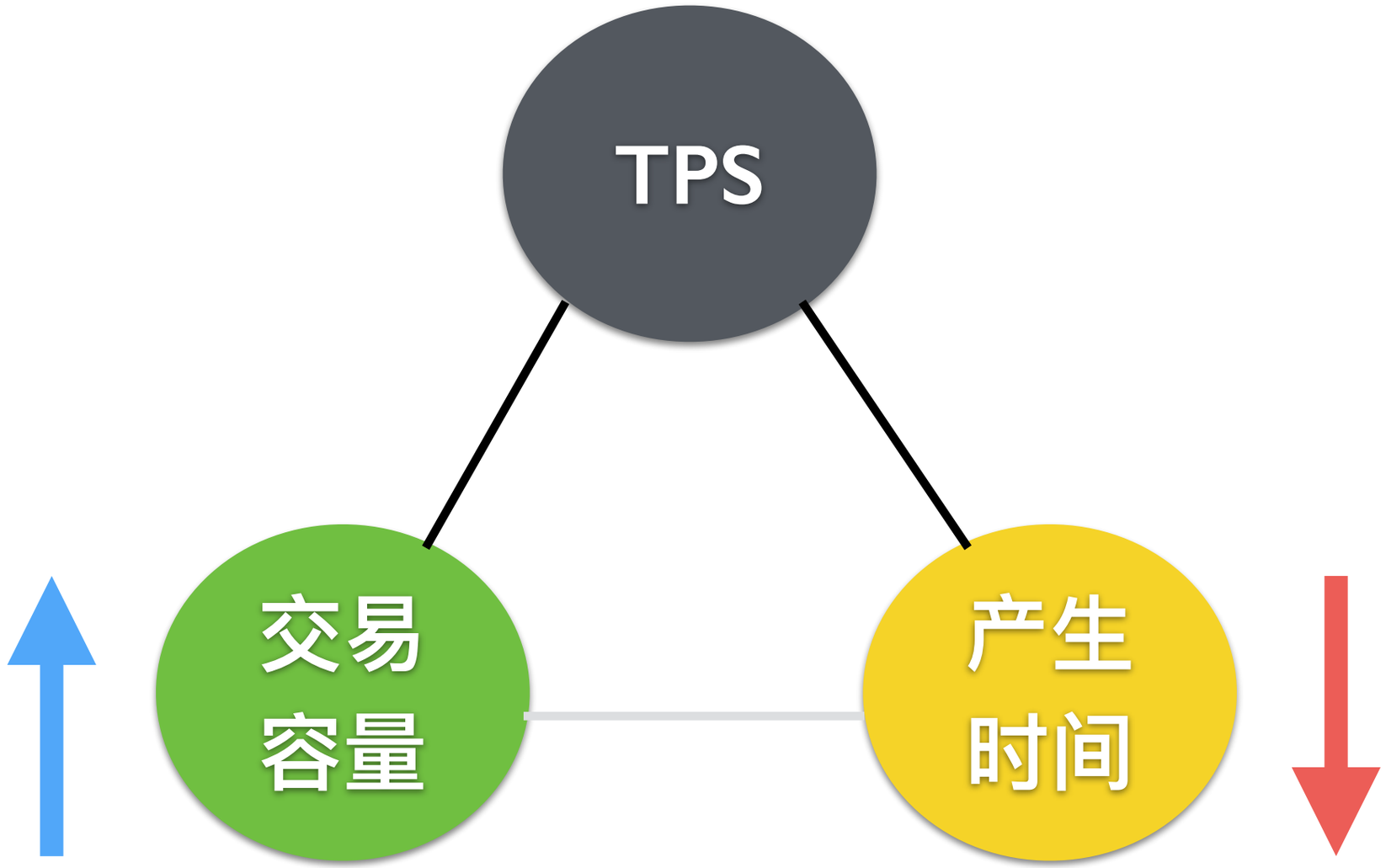
https://tradeblock.com/bitcoin/historical/1d-f-tsize_per_avg-00271



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

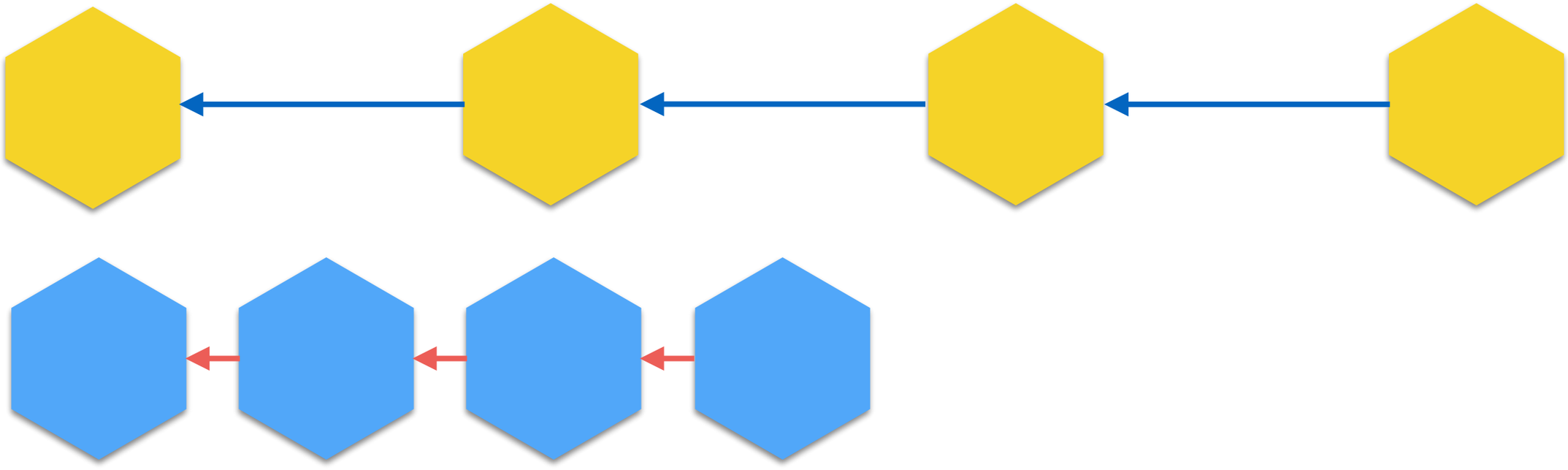
减少块产生时间

块传播时间

块产生时间

块传播时间

块产生时间



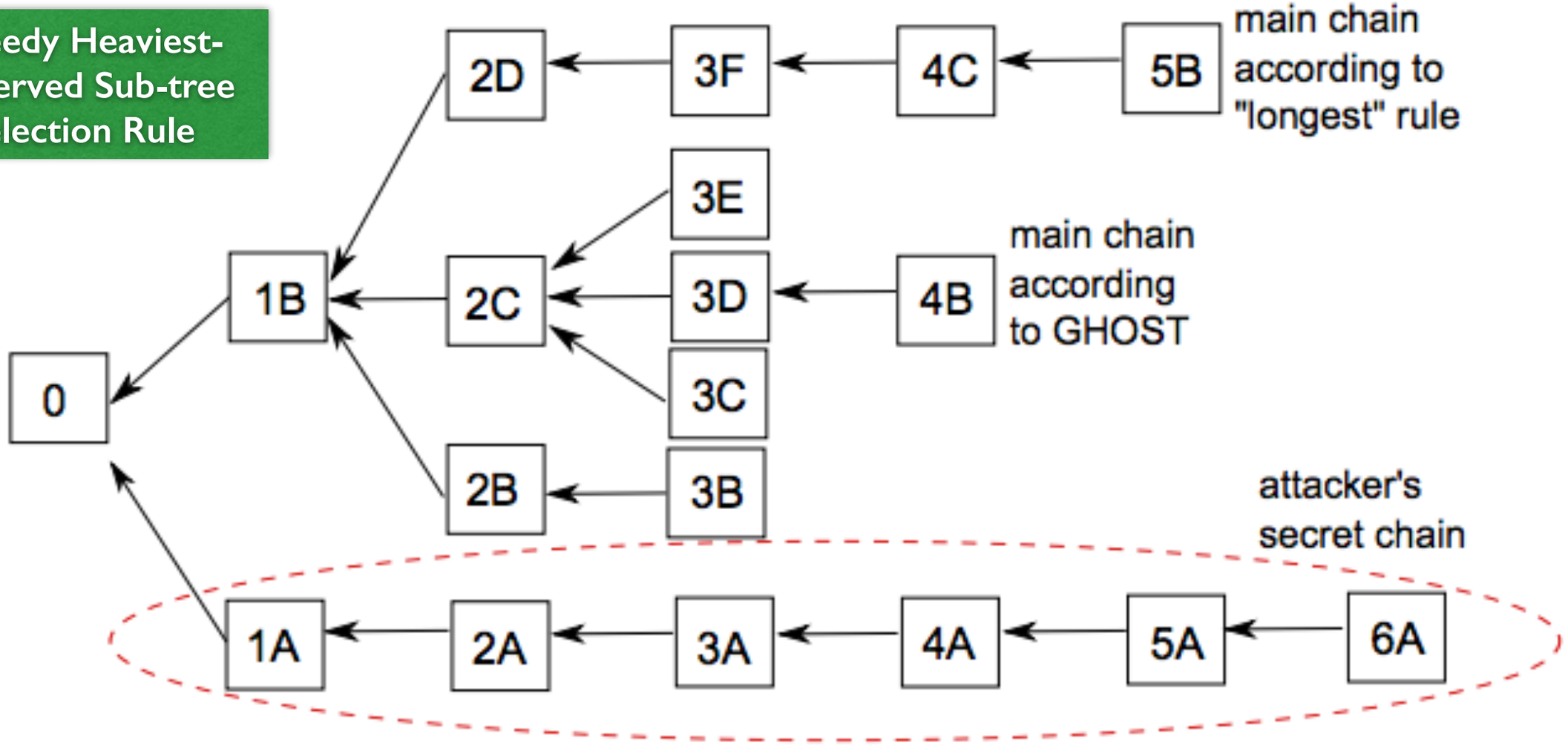
GHOST协议

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

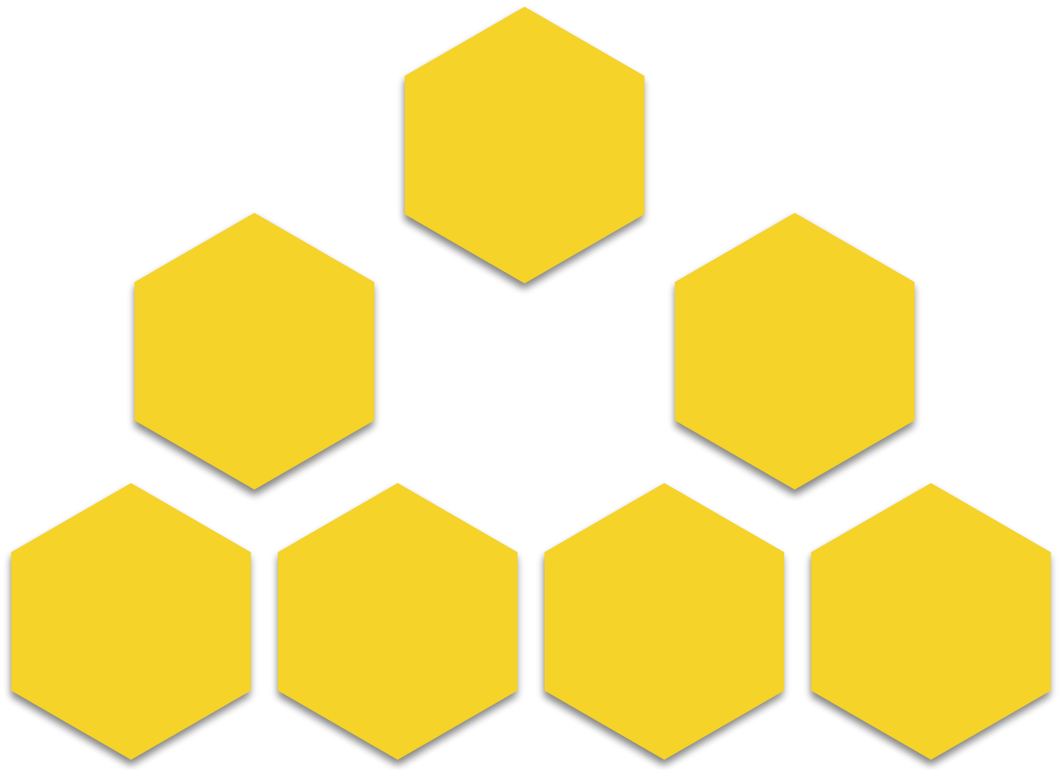
Secure High-Rate Transaction Processing in Bitcoin

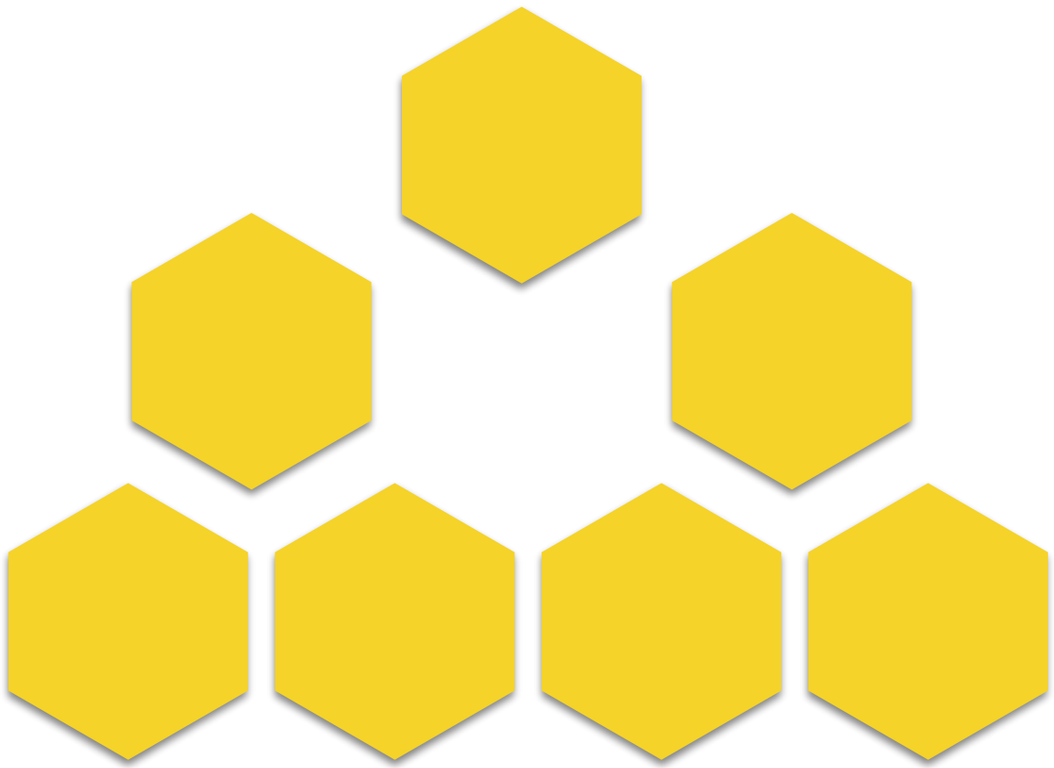
Financial Cryptography and Data Security 2015

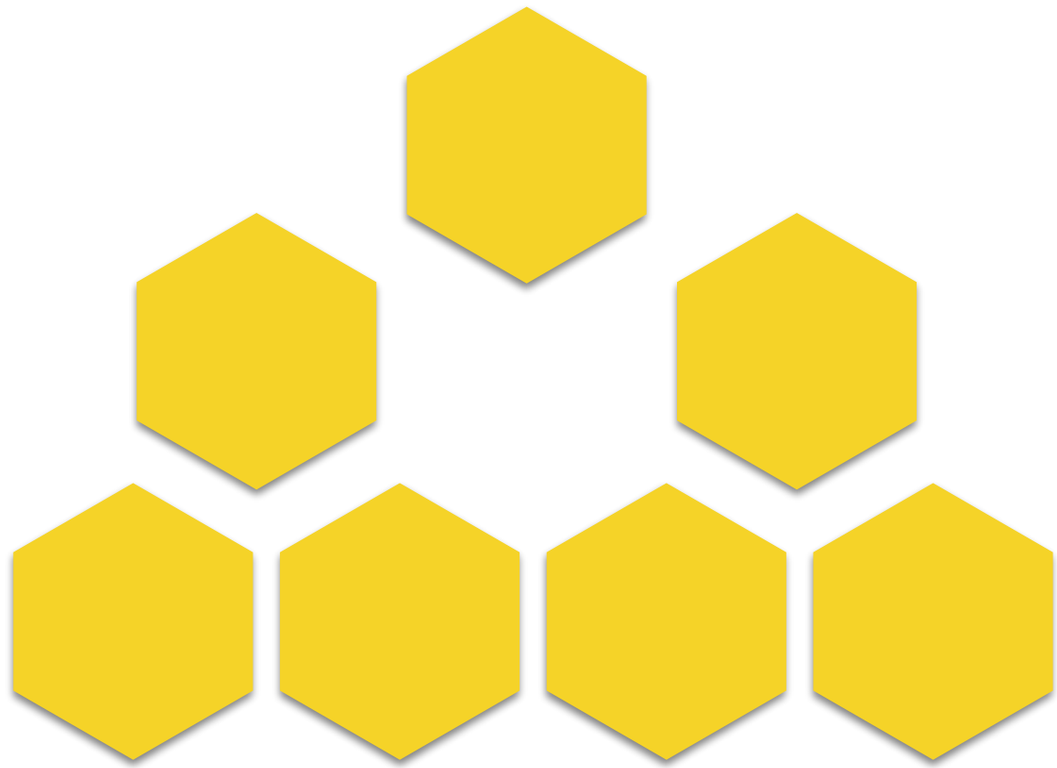
Greedy Heaviest-Observed Sub-tree selection Rule



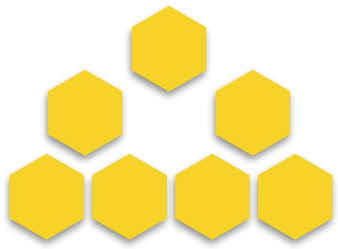
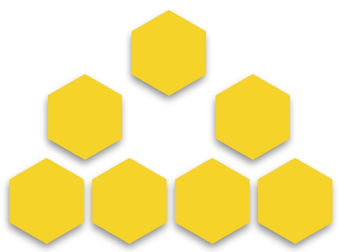
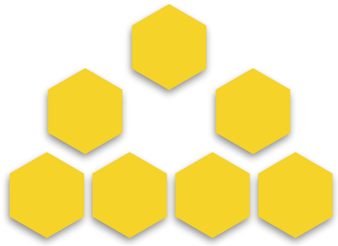
增大块大小







增大块大小

容易执行

更低的成本

矿工同意即可

硬分叉

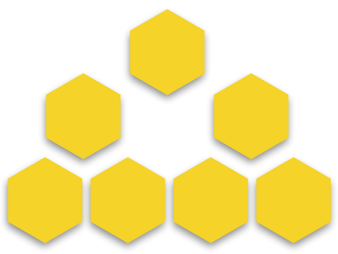
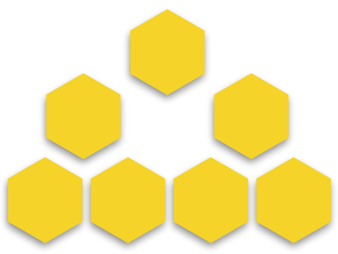
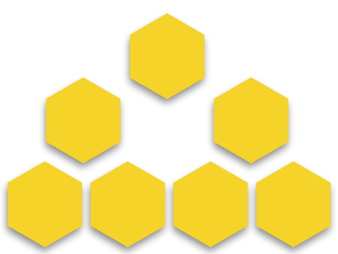
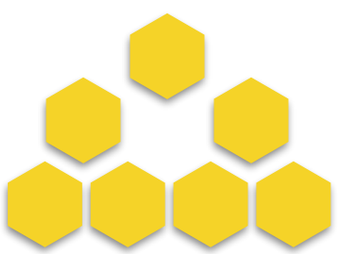
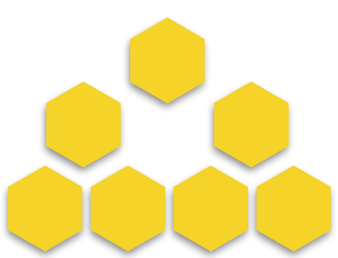
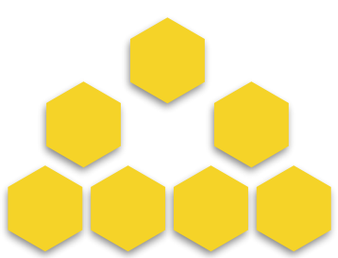
计算能力

更长的传播时间

大小增长块

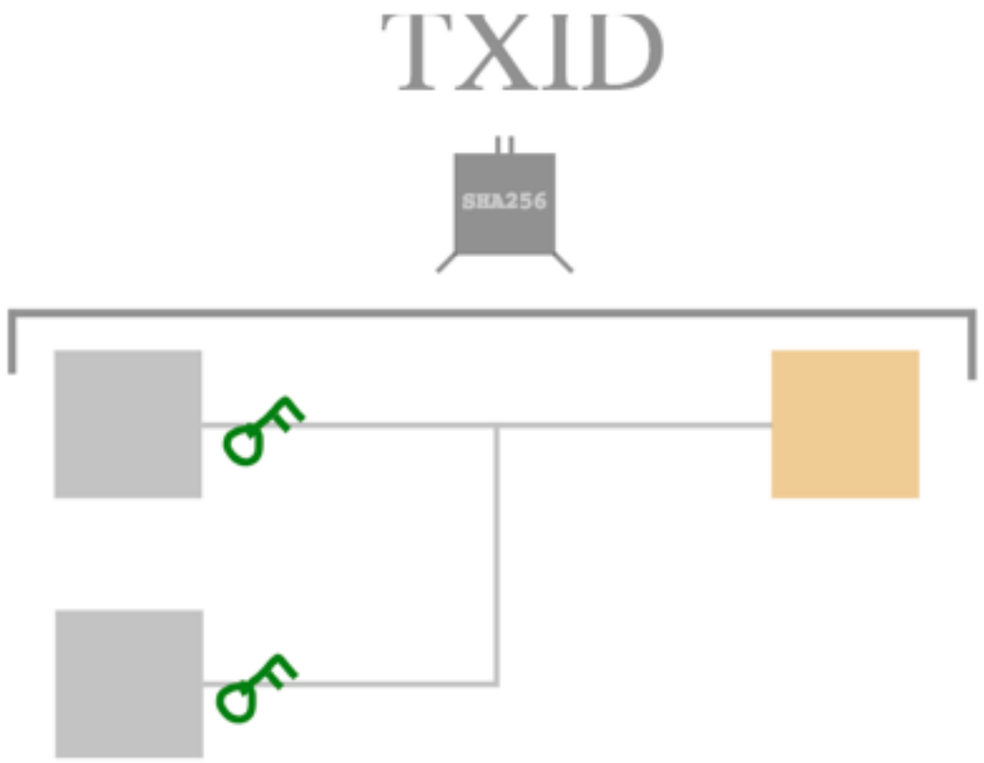
挖矿设备

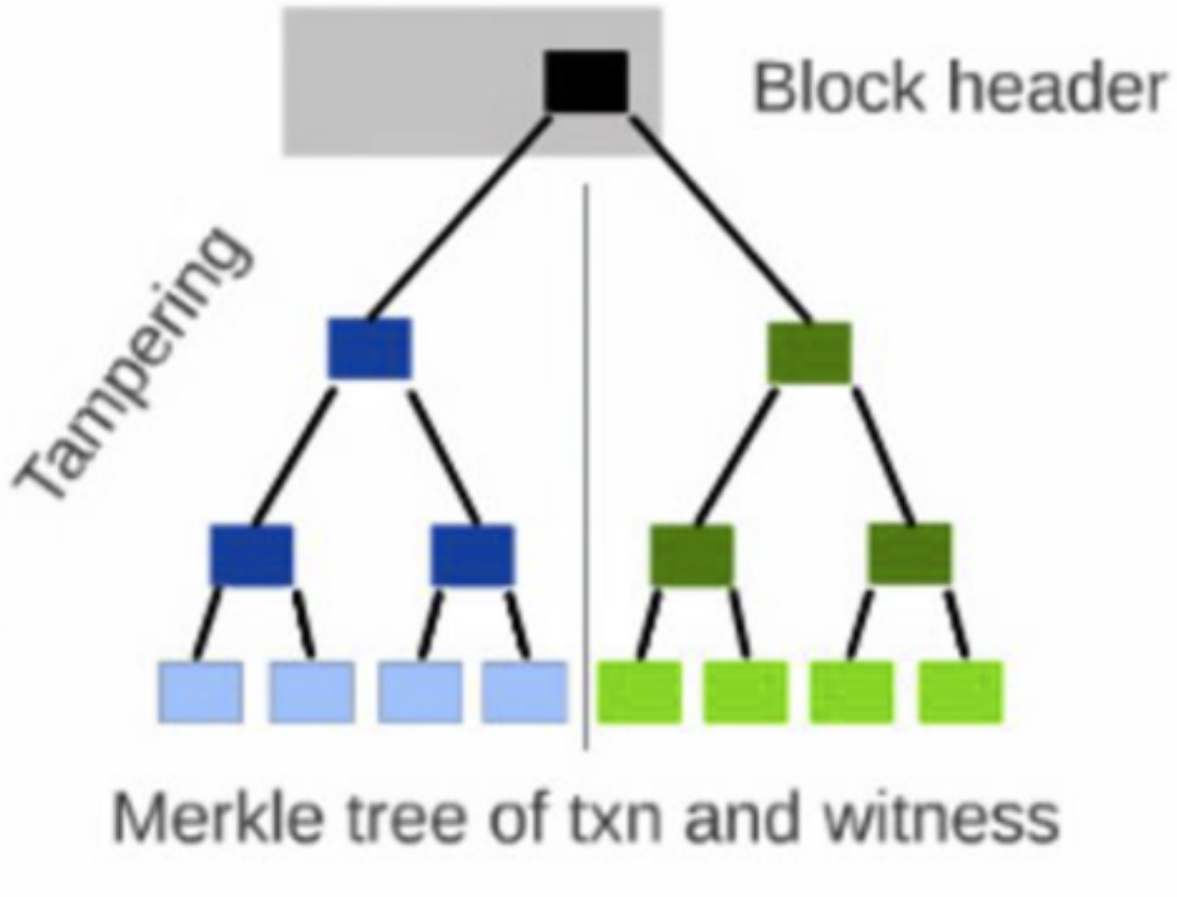
安全性

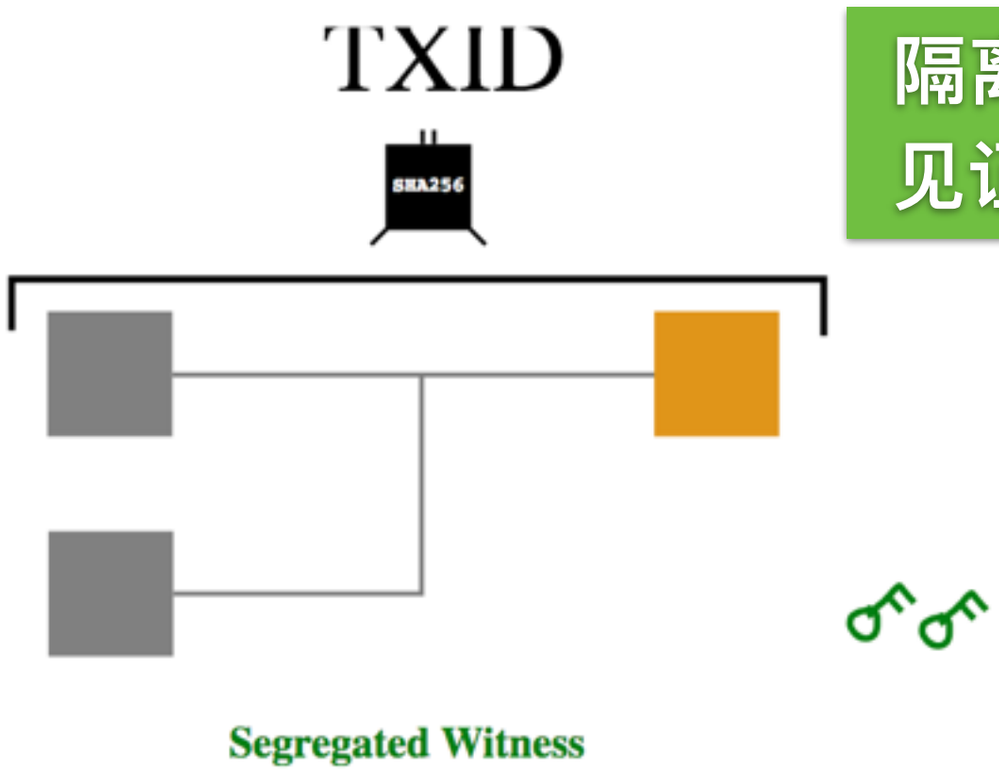







减少交易大小

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





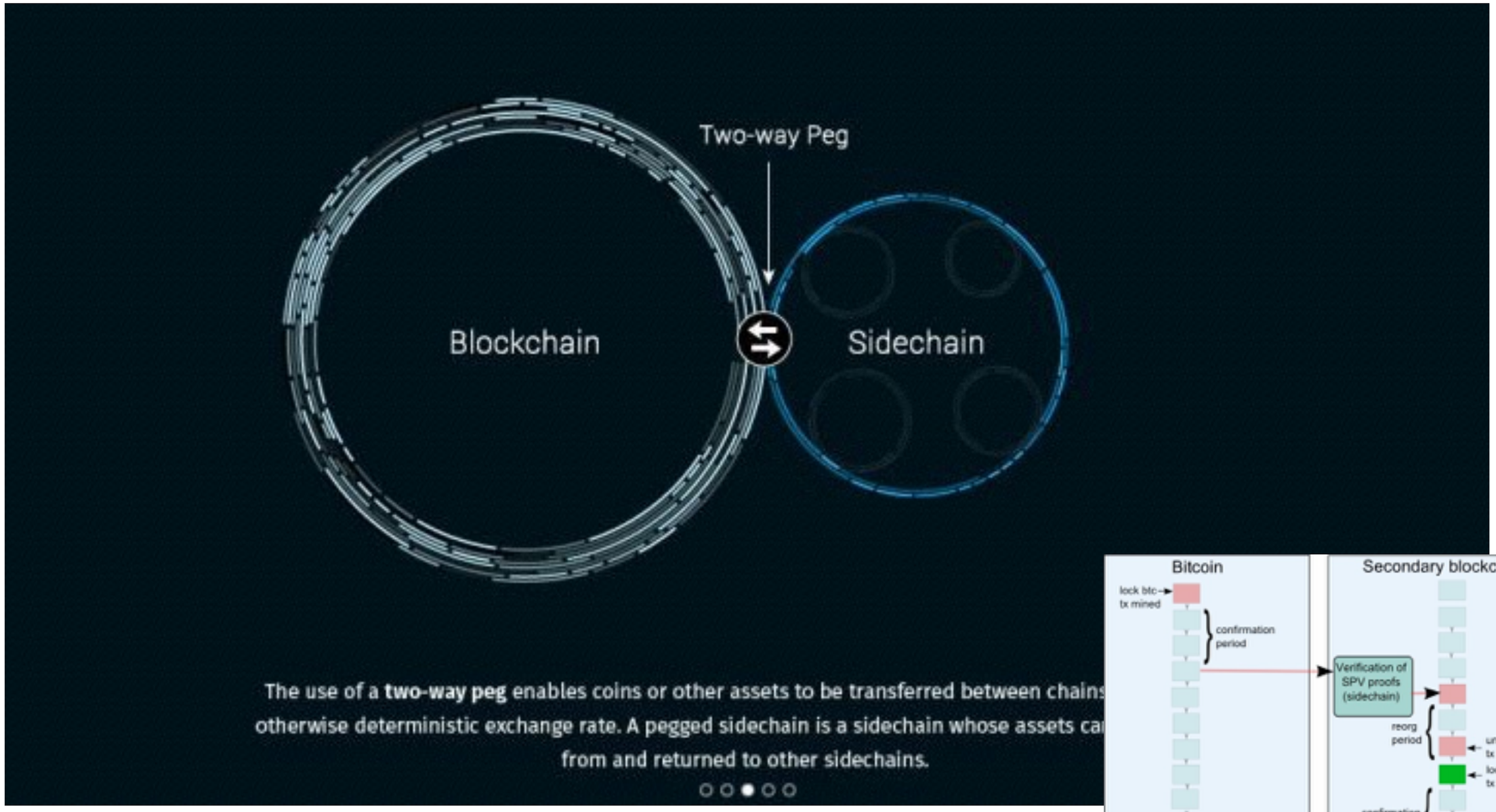


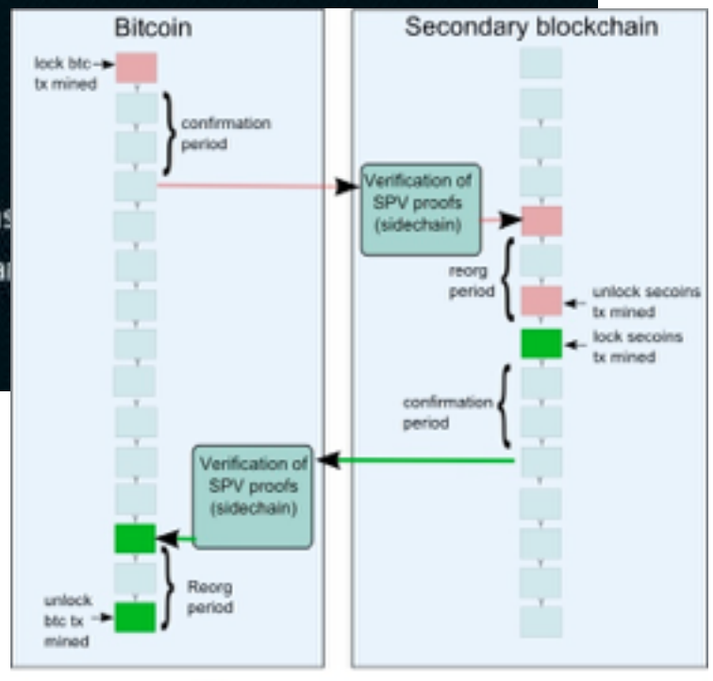
隔离见证

优点

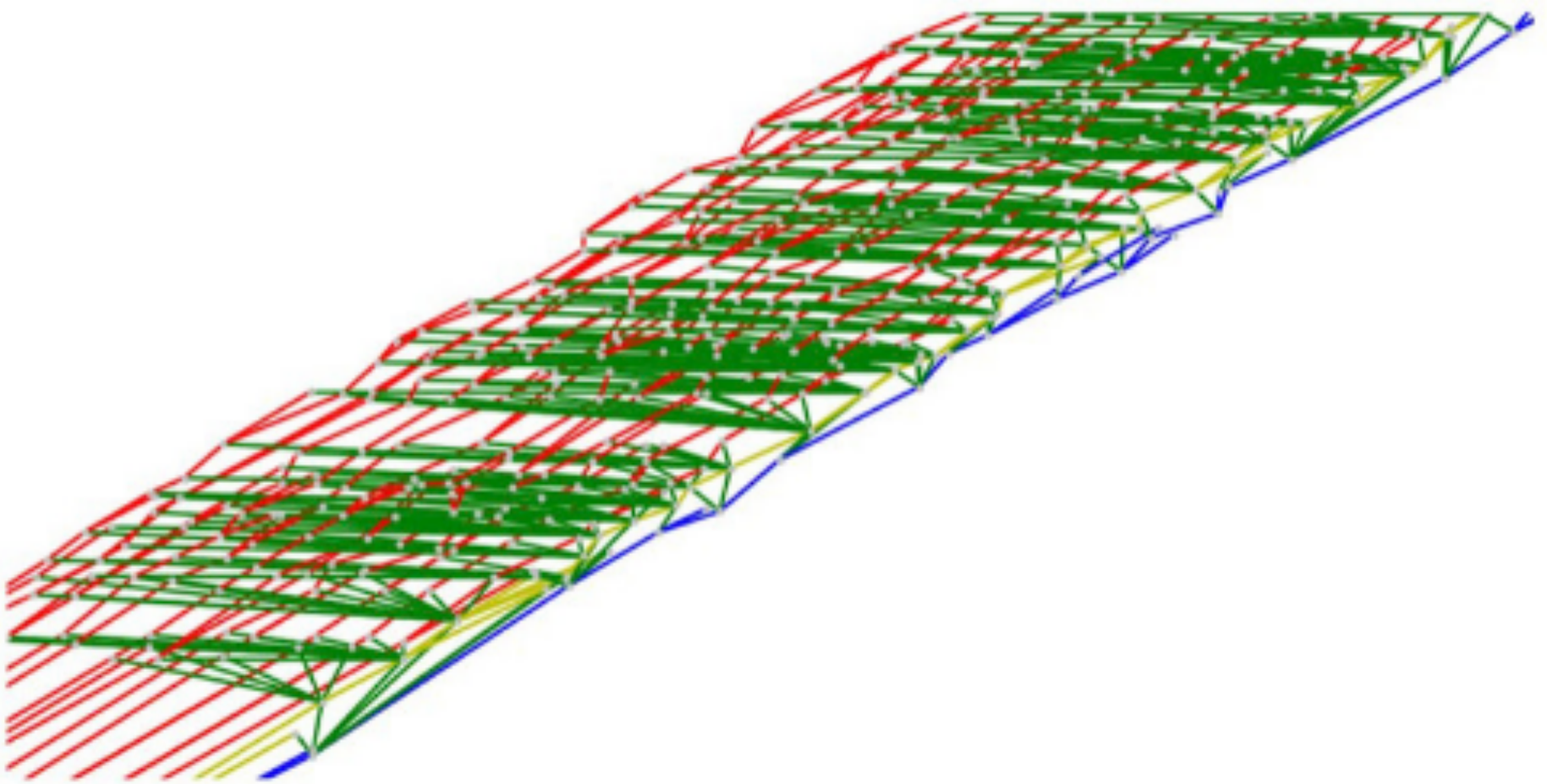
缺点

侧链

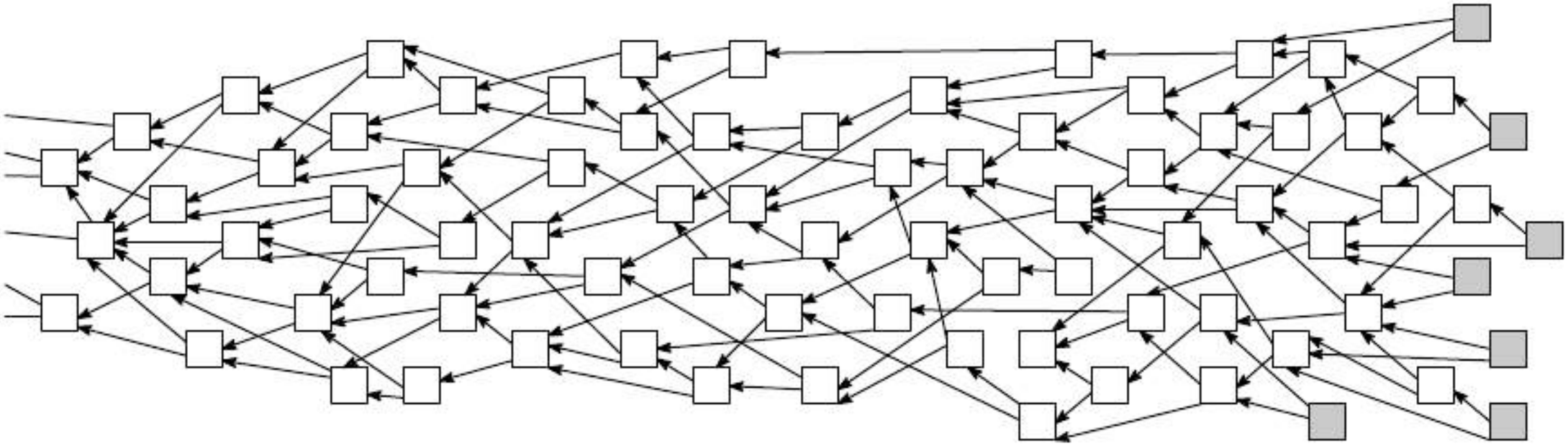

Two-way Peg
Blockchain
Sidechain
The use of a **two-way peg** enables coins or other assets to be transferred between chains
otherwise deterministic exchange rate. A pegged sidechain is a sidechain whose assets ca
from and returned to other sidechains.


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

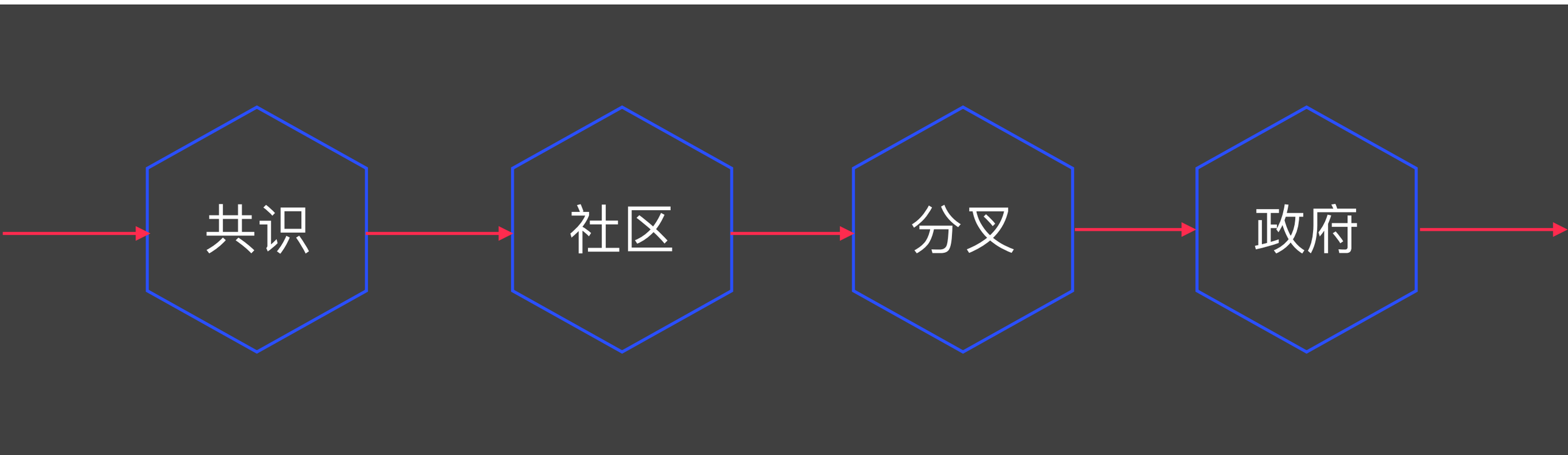
分片



DAG



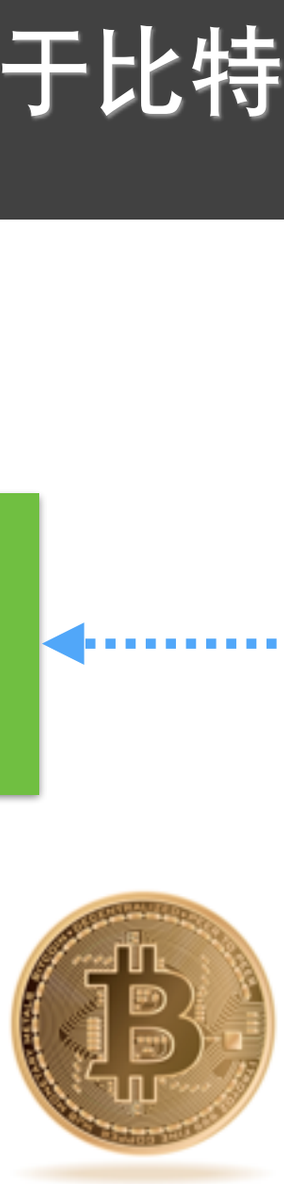
监管



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

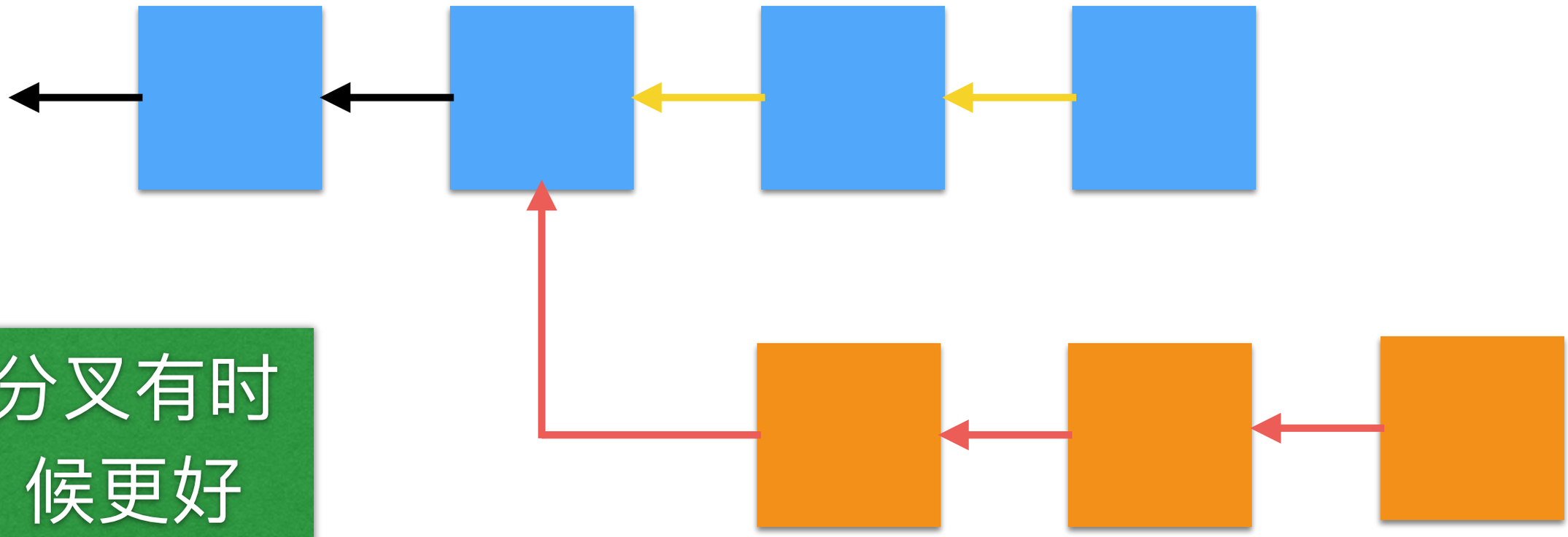
投资人：购买

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

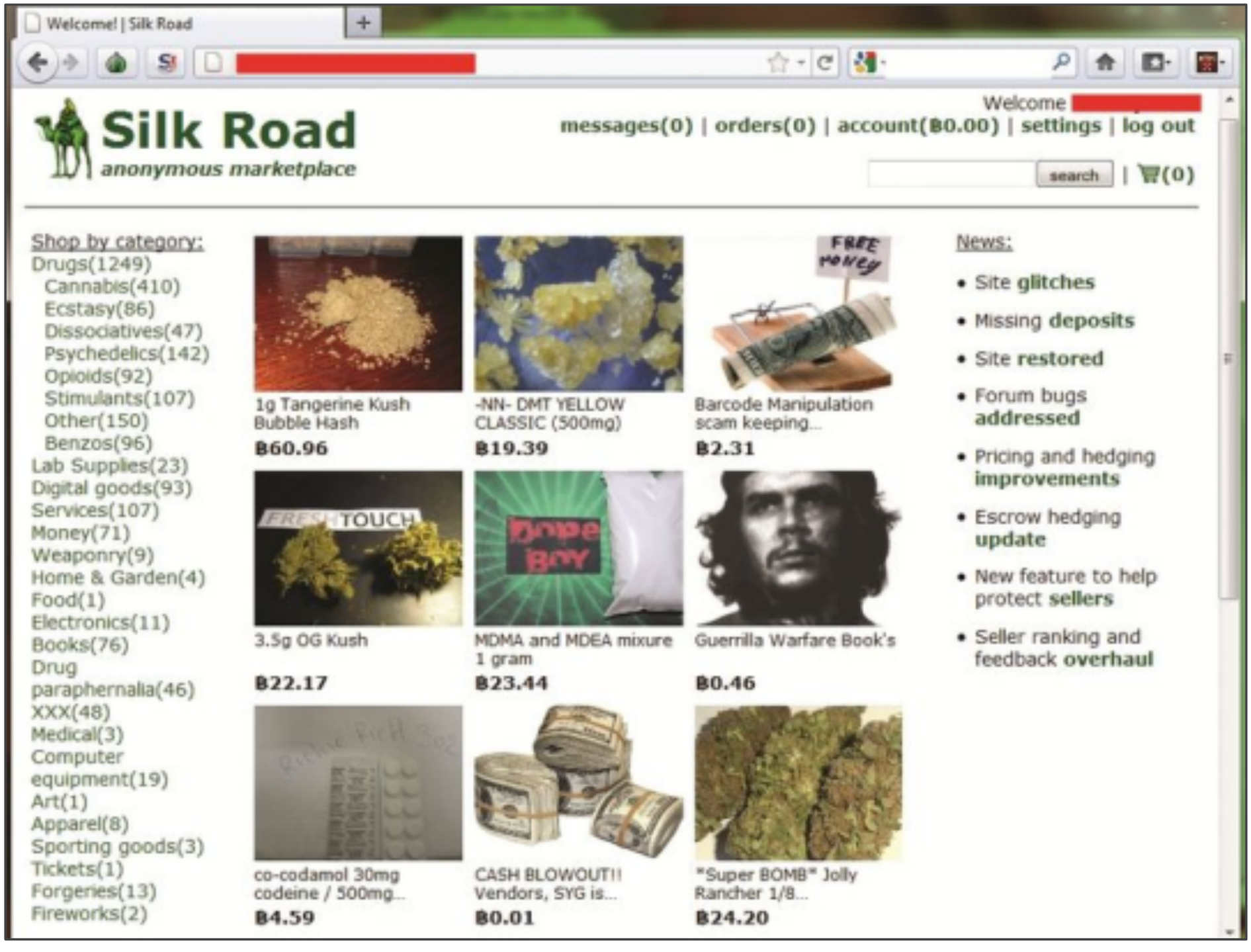
纽约州比特币牌照

美国加密货币管理政策

中国政府2017年系列政策

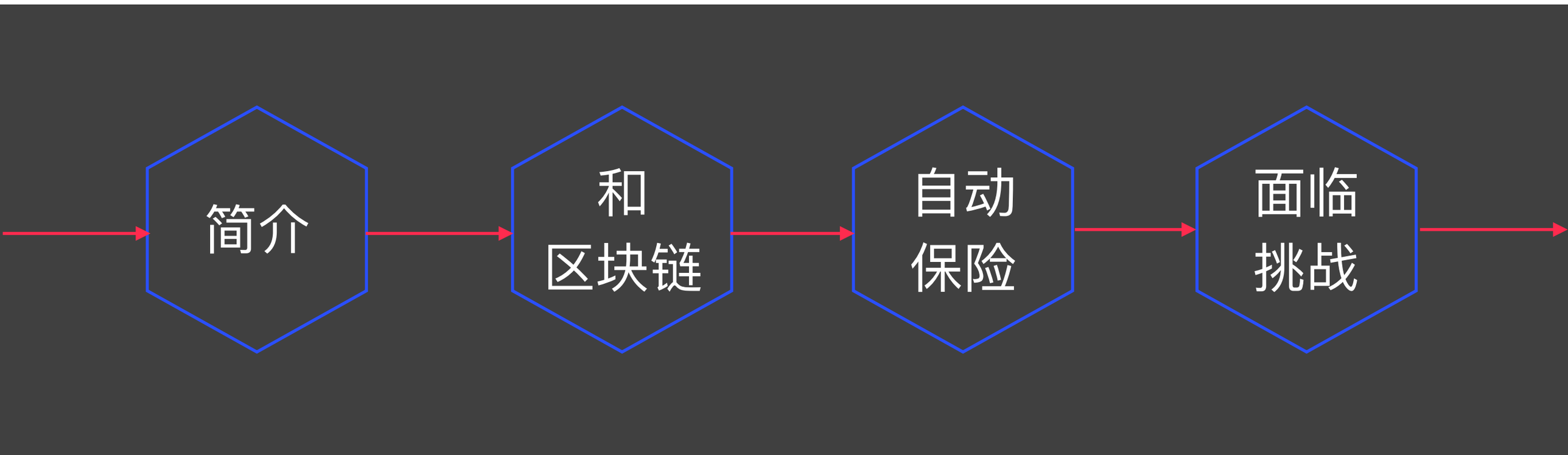
日韩新加坡

丝绸之路



把现实世界和虚拟世界完全分离开是很困难的

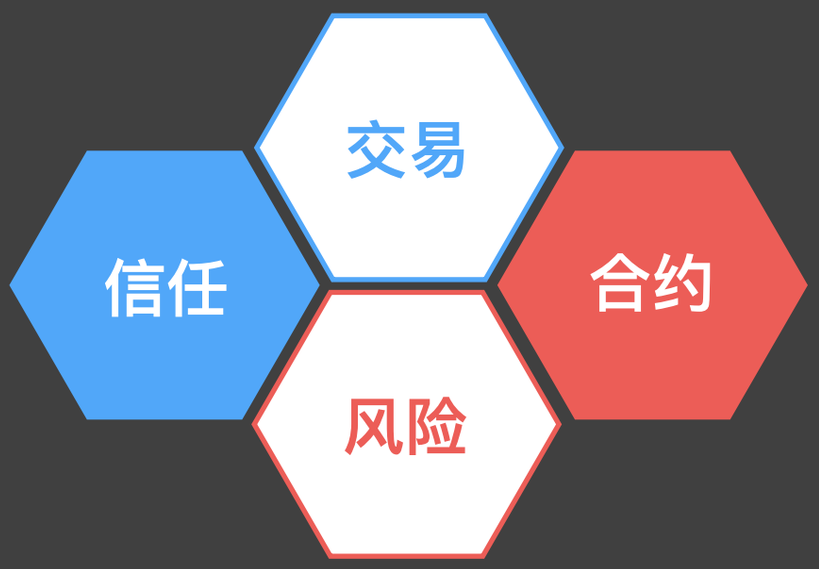
智能合约



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

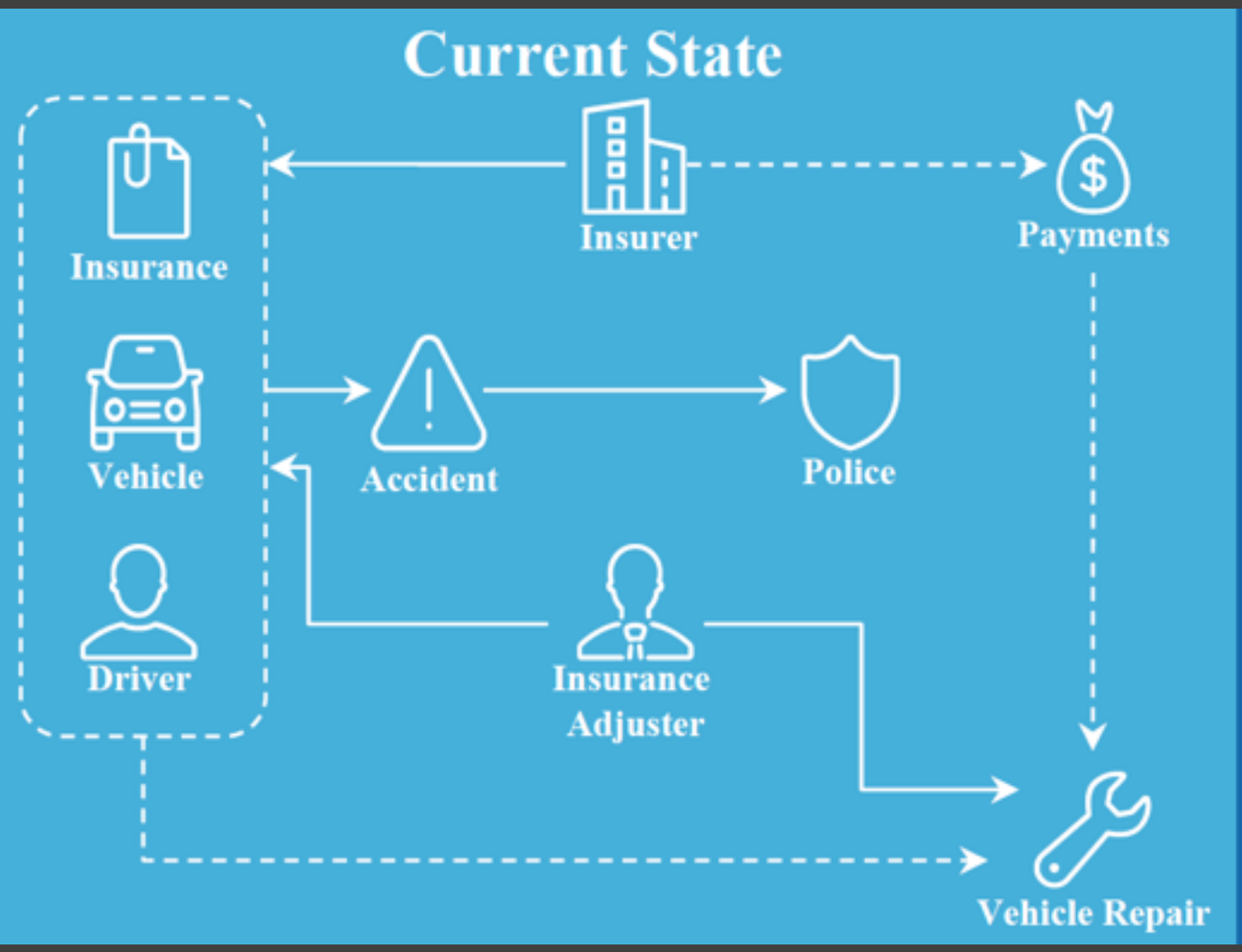
智能合约在区块链上存储并执行

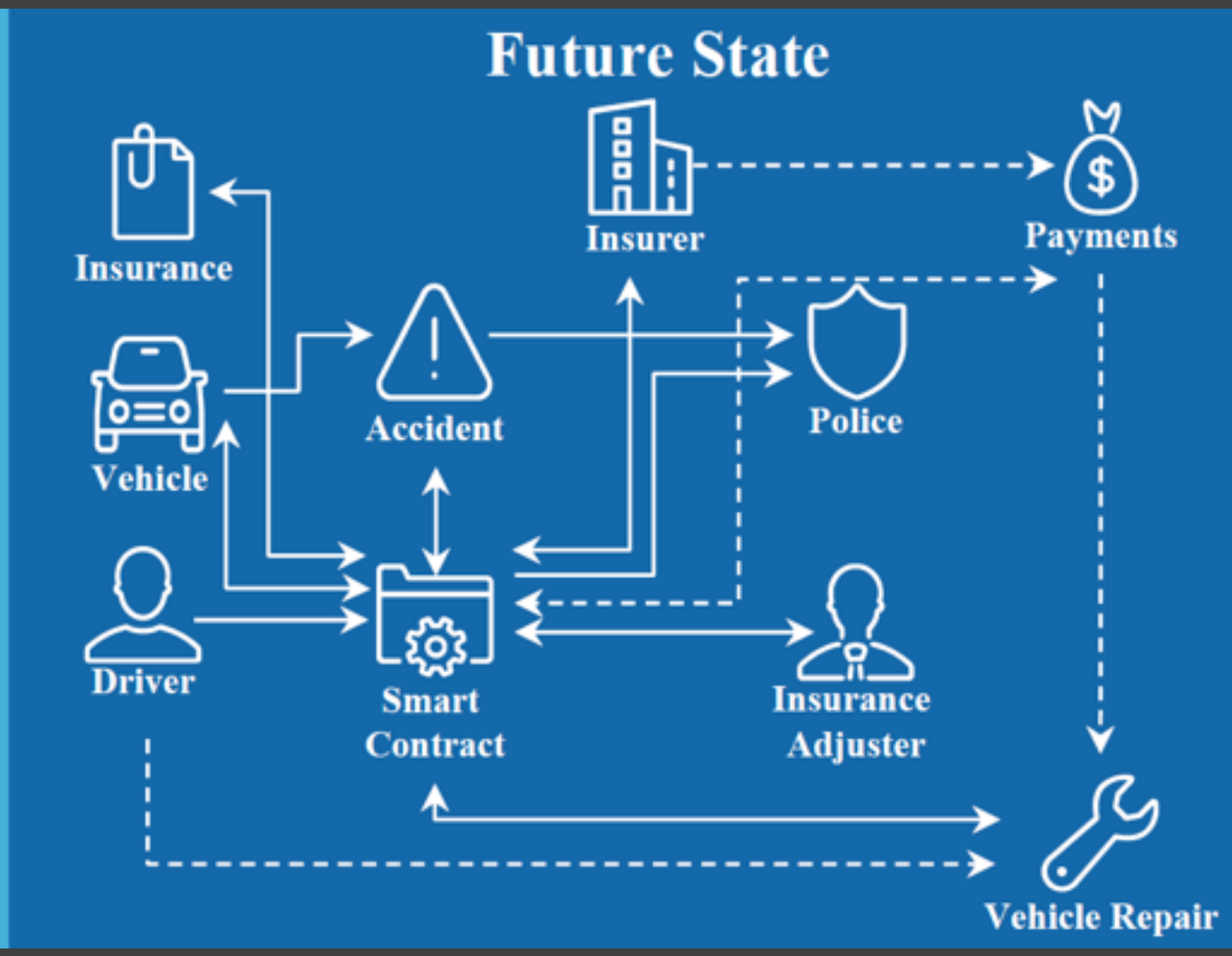
Block #FCAC
prev #618C
</> contract 2E12…
</> contract FECB…
</> contract 21E0…
…

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

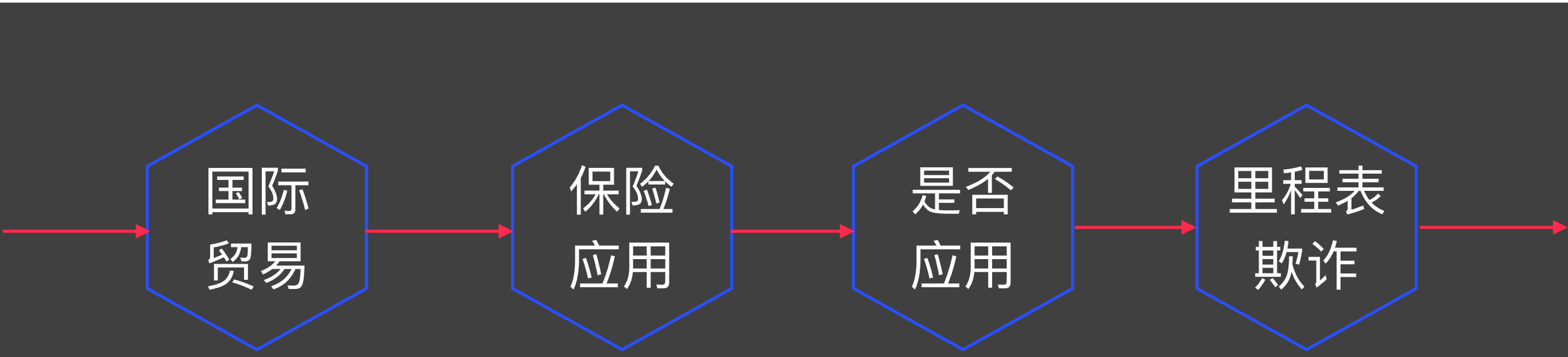
安全

- 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

区块链应用



Blockchain II

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；

应用场景

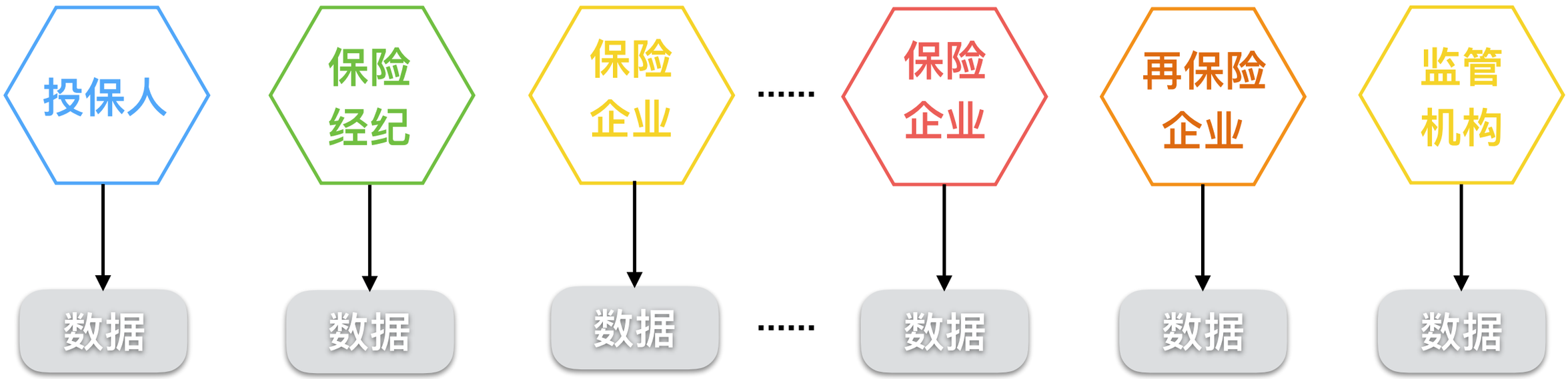
使用区块链来更新改造传统的外贸信用证、外贸保函、福费廷、保理和票据等业务。

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



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

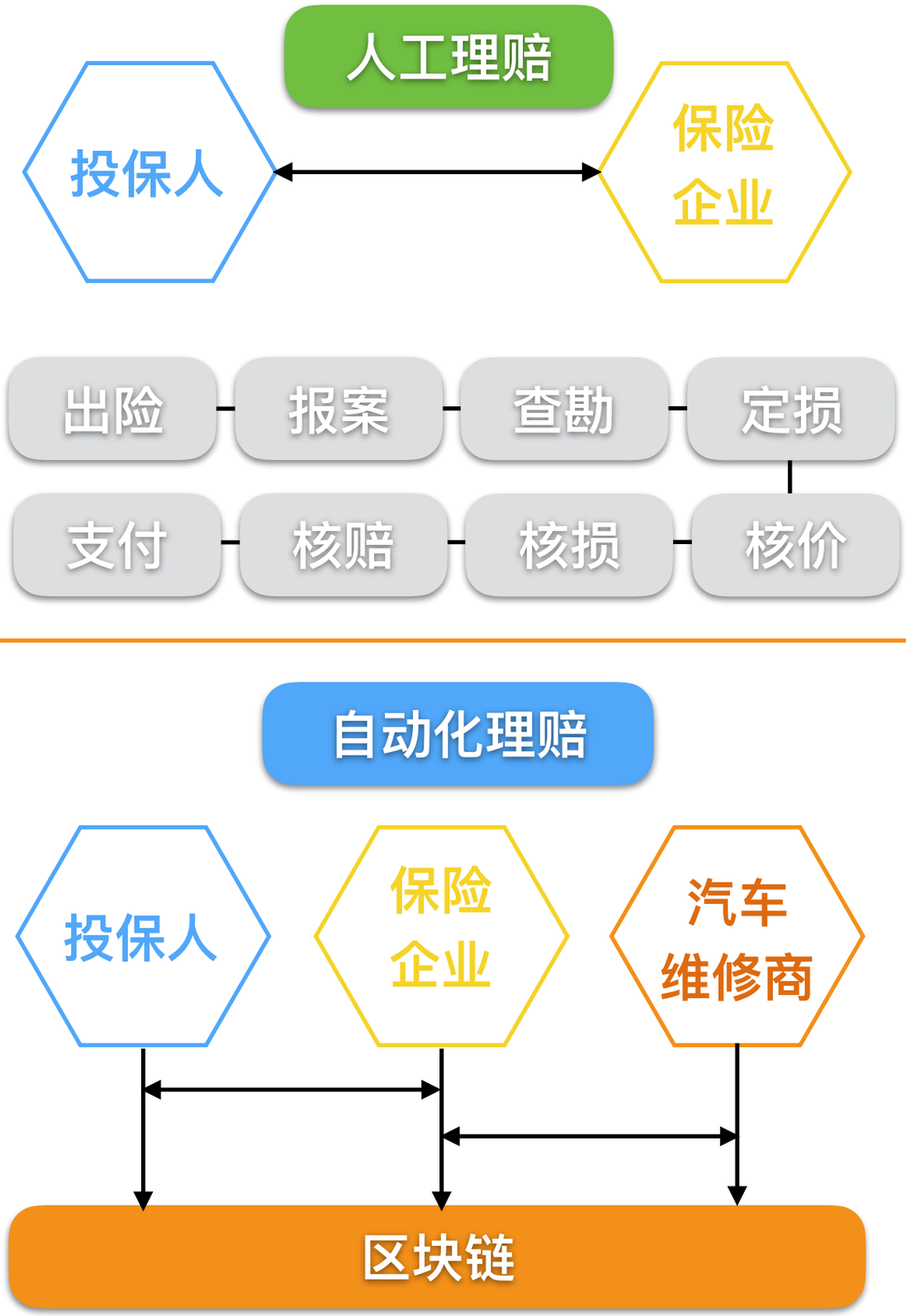
AI

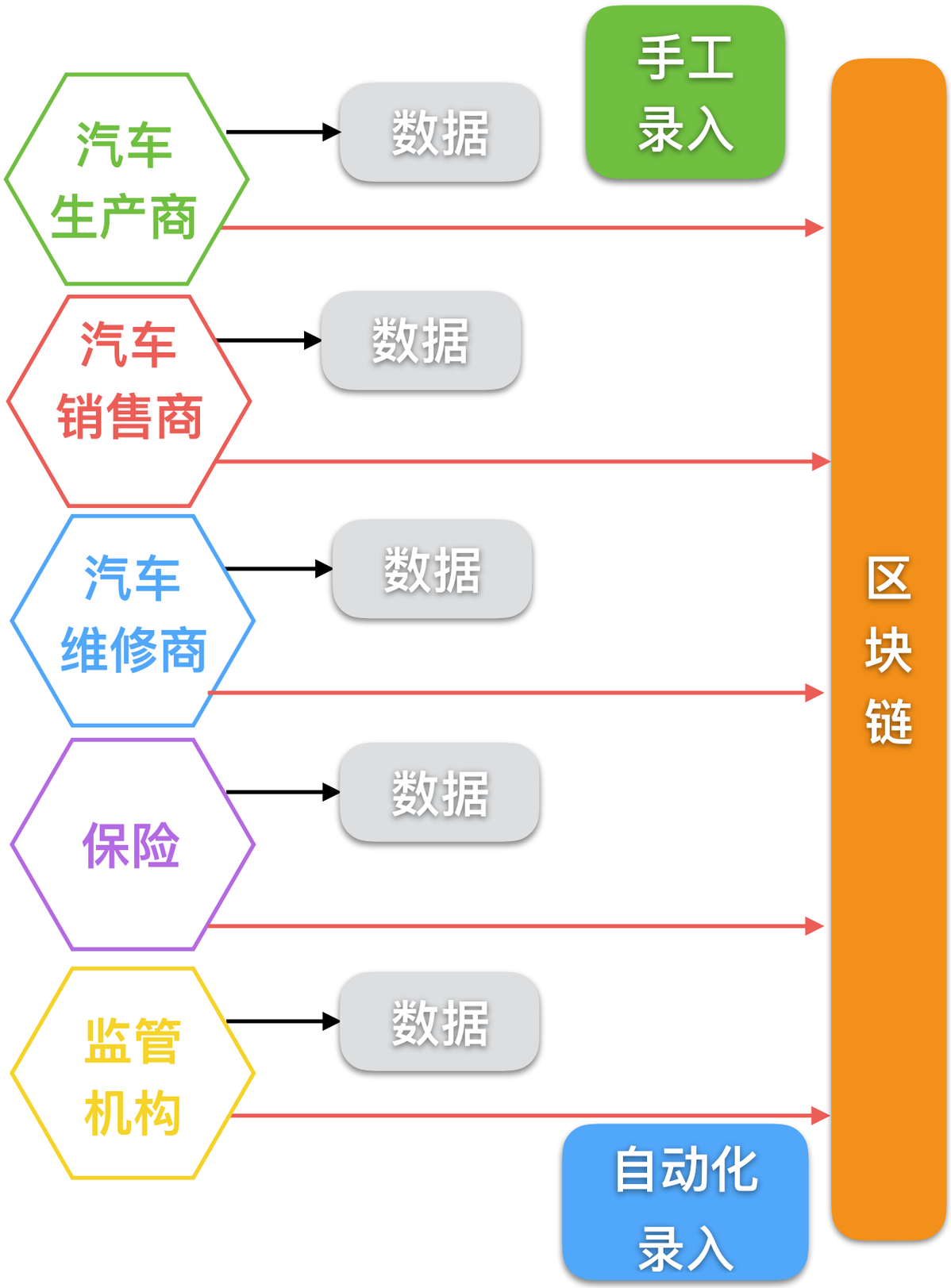
BigData

Cloud

Blockchain

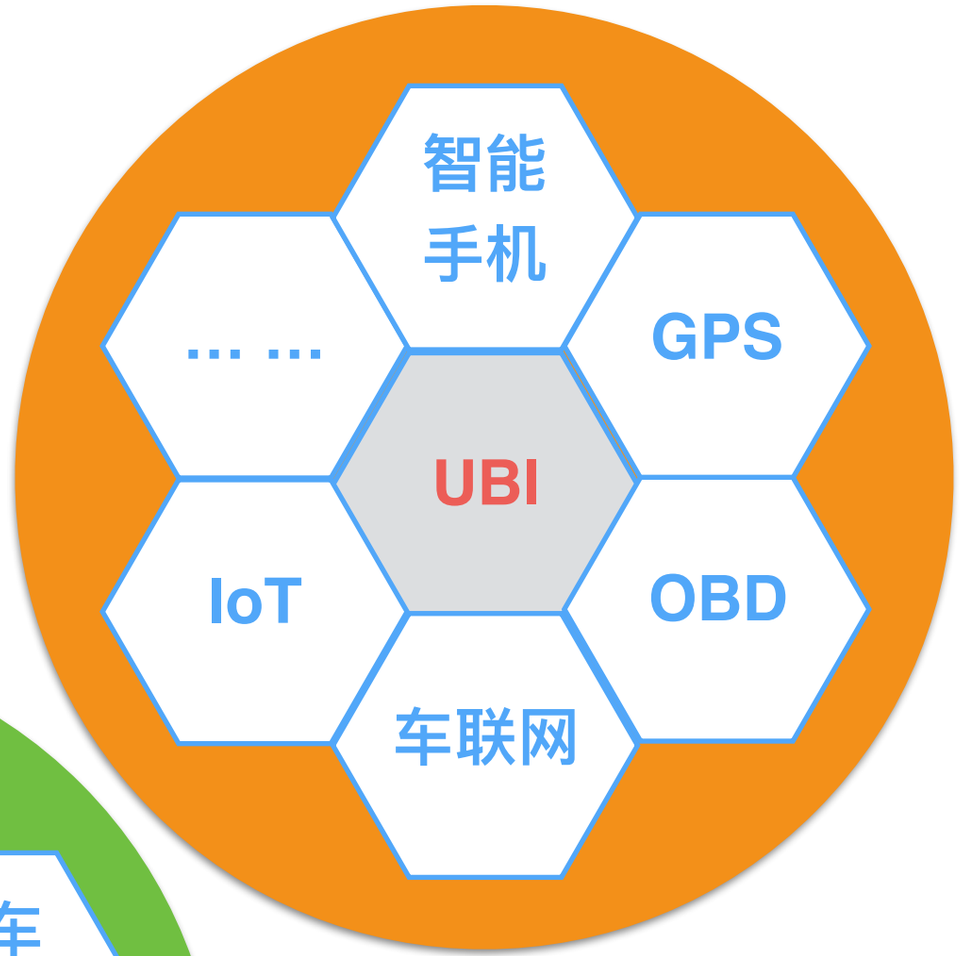
自动化


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

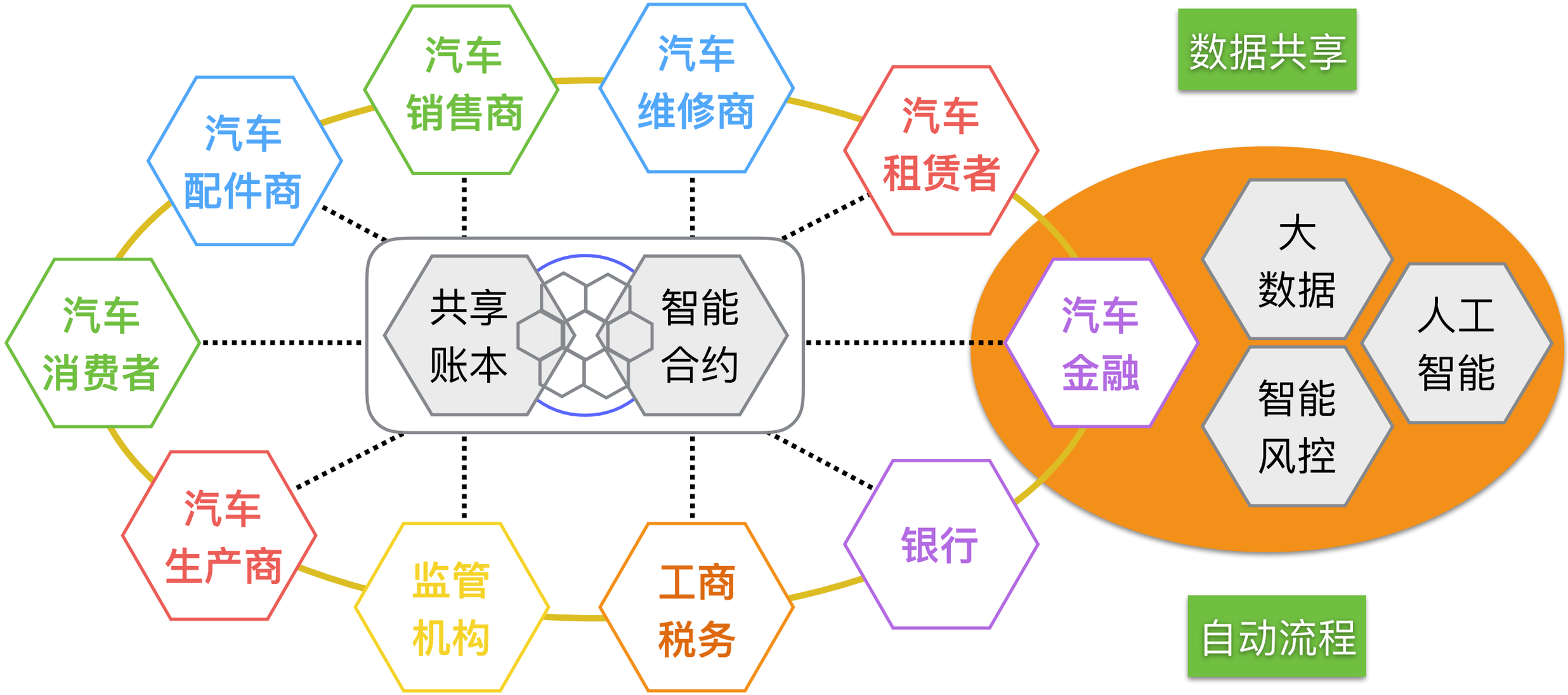
定价


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

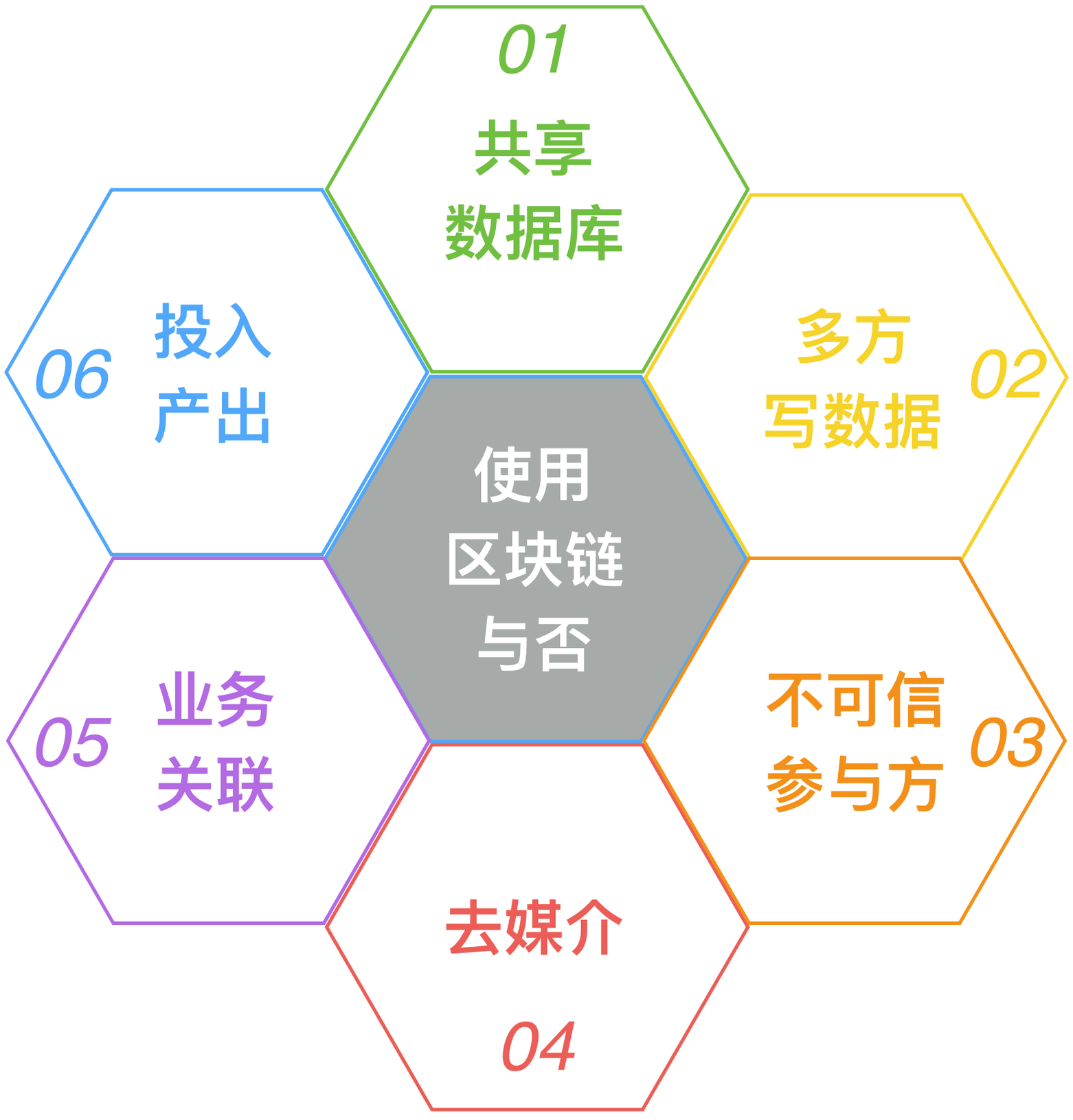
防欺诈



基于多来源数据
比对防欺诈

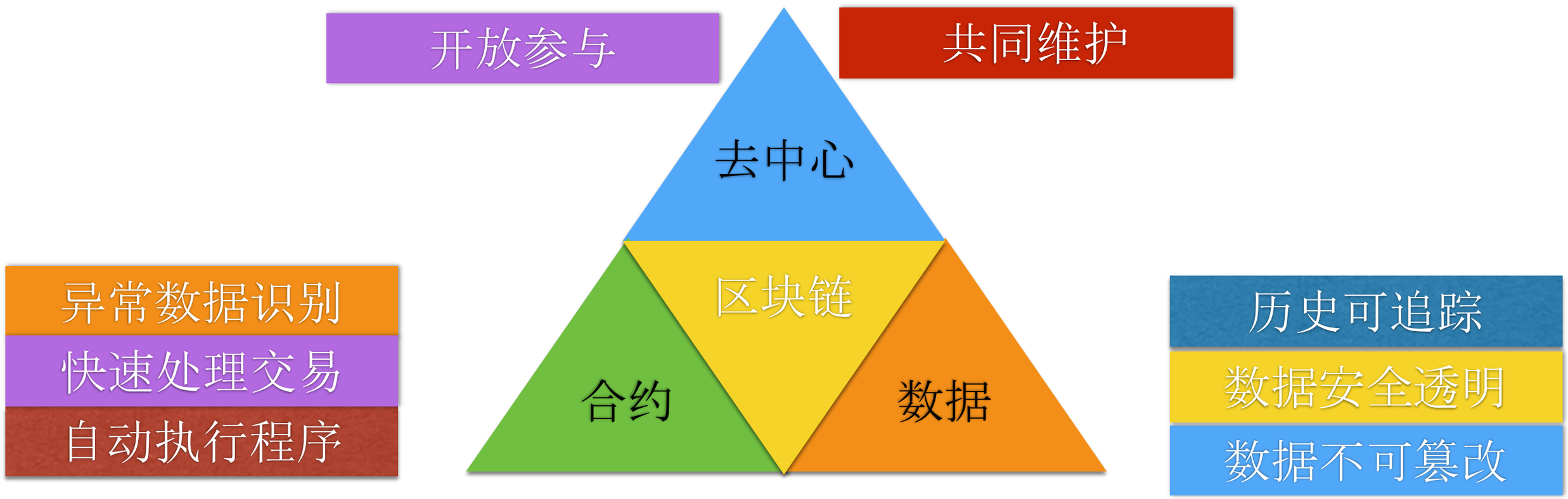
基于自动化和智能
合约防欺诈

是否需要使用区块链



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

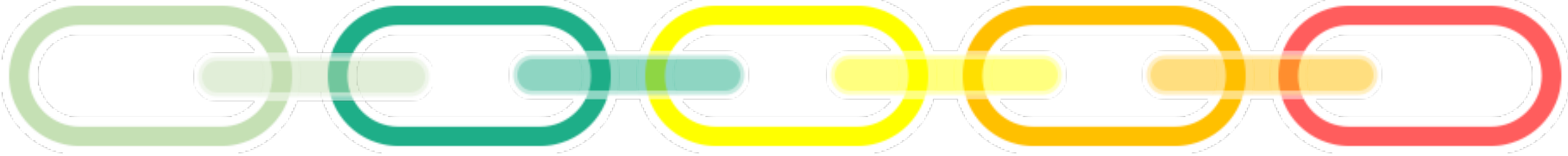

开放参与
共同维护
去中心
区块链
合约
数据
异常数据识别
快速处理交易
自动执行程序
历史可追踪
数据安全透明
数据不可篡改

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。

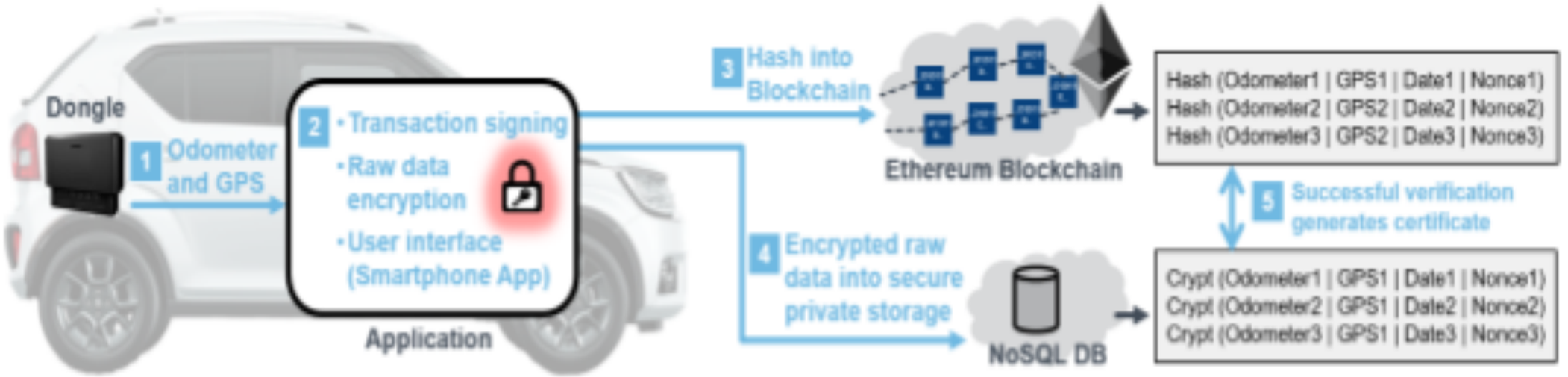
保险公司：保险公司拥有汽车保险信息，以及通过保险理赔的事故信息和维修记录。

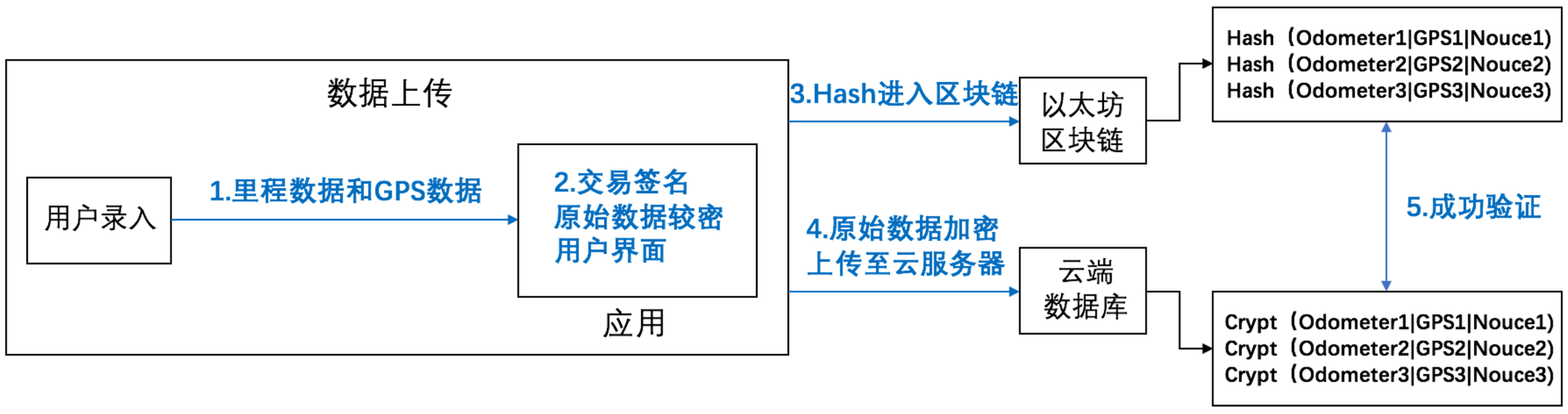


汽车使用者：通过车载远程设备是记录汽车数据，主动规律得上传汽车的使用情况，比如里程、gps、油耗、车速等。或允许用户手动录入。

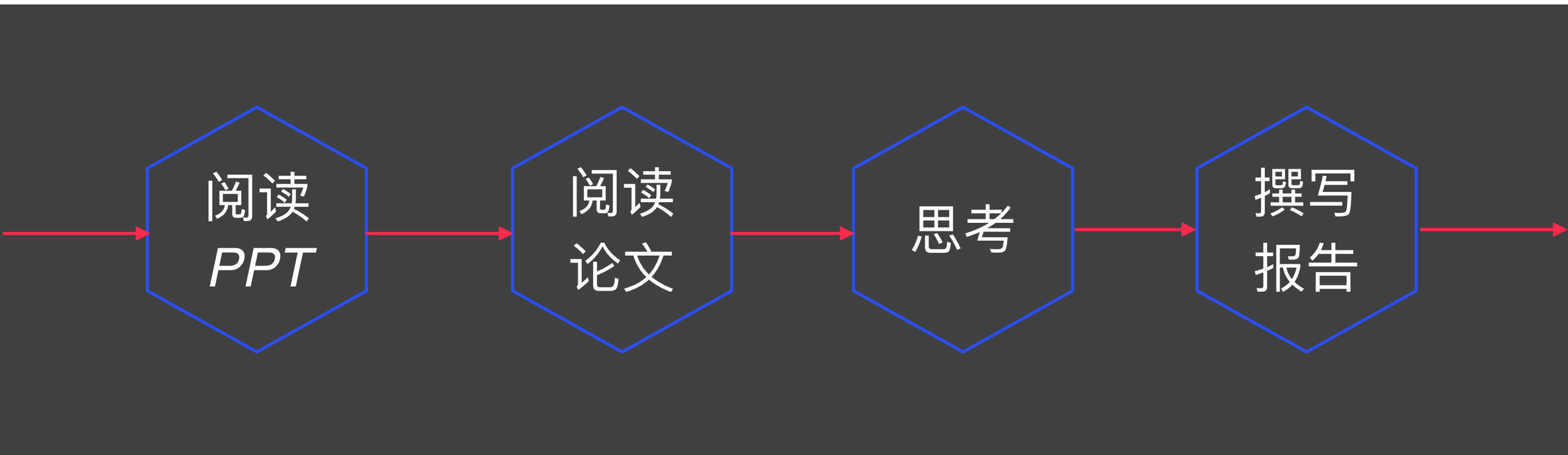
汽车服务商和服务站：汽车在进行维修时，维修站向相关部门提交汽车的数据，汽车服务商收集的数据，可以与其它渠道的数据相互印证。

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
4 Encrypted raw data into secure private storage
NoSQL DB
Hash (Odometer1 | GPS1 | Date1 | Nonce1)
Hash (Odometer2 | GPS2 | Date2 | Nonce2)
Hash (Odometer3 | GPS2 | Date3 | Nonce3)
5 Successful verification generates certificate
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

要求阅读如下论文，写论文阅读报告

In IEEE SP 2015

2015 IEEE Symposium on Security and Privacy

SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies

Joseph Bonneau*†‡, Andrew Miller§, Jeremy Clark¶, Arvind Narayanan*, Joshua A. Kroll*, Edward W. Felten*
*Princeton University, †Stanford University, ‡Electronic Frontier Foundation, §University of Maryland, ¶Concordia University

https://ieeexplore.ieee.org/document/7163021

选择一篇引用该文的论文，阅读该论文
并在论文阅读报告中简单介绍

1、论文概述
2、主要收获
3、存在疑问
4、所思所感
5、一篇引用

12月20日晚上
12点前提交

谢谢！

Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io