比特币介绍

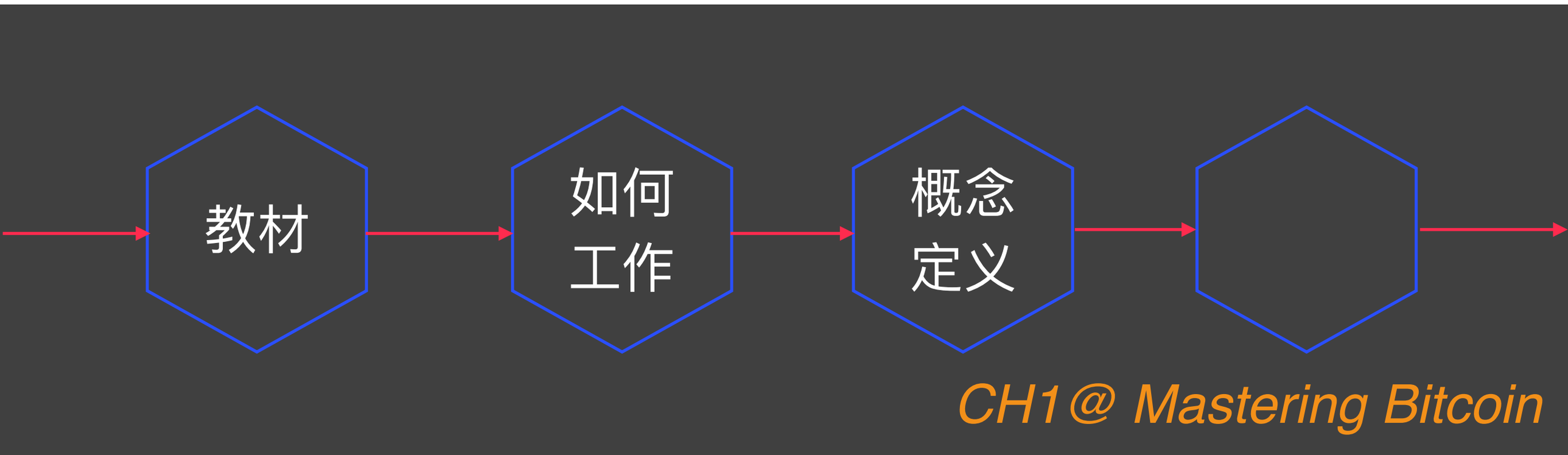
北京大学 软件与微电子学院
School of Software and Microelectronics, Peking University

Huiping Sun(孙惠平)
sunhp@ss.pku.edu.cn

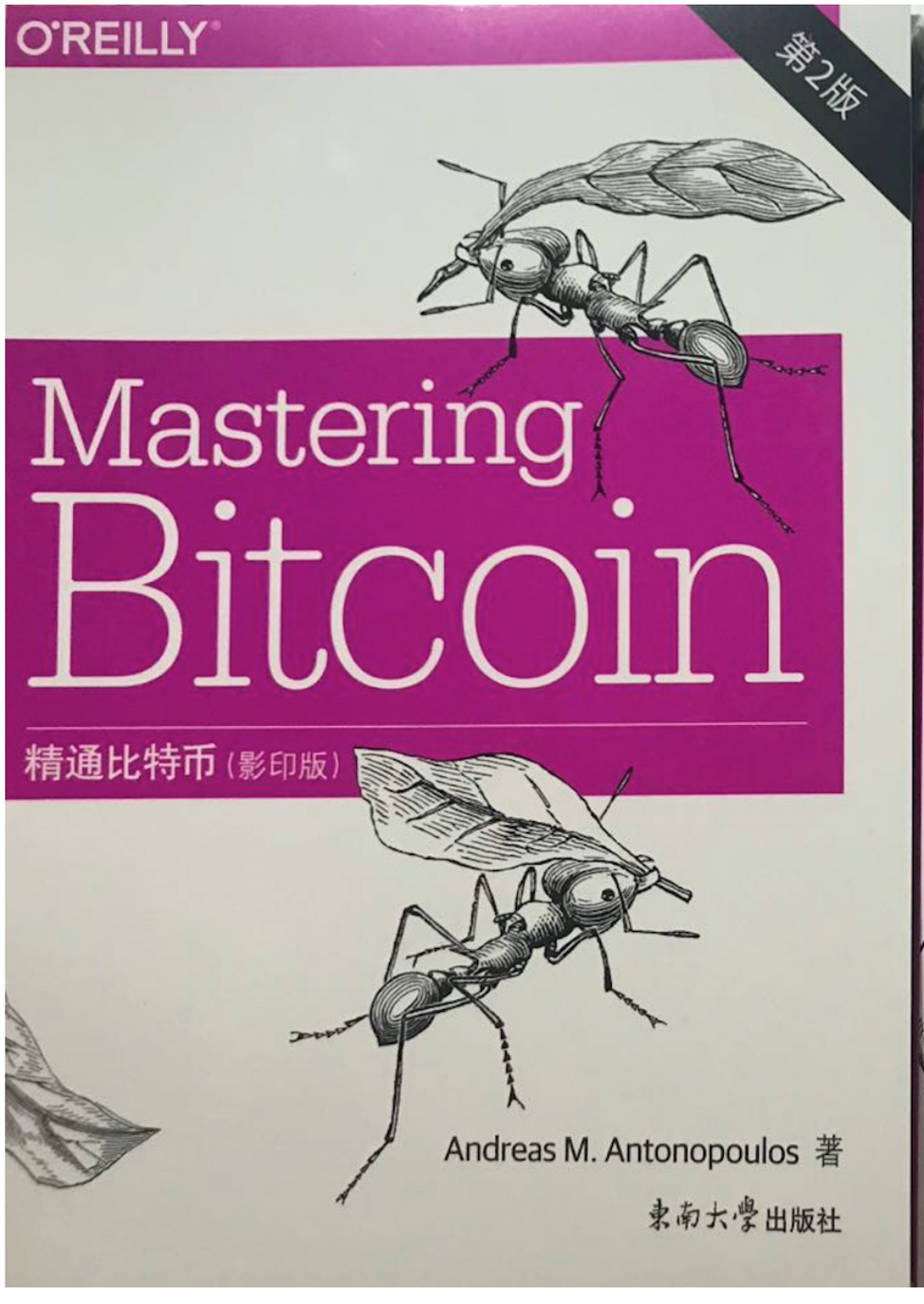
上次课程内容

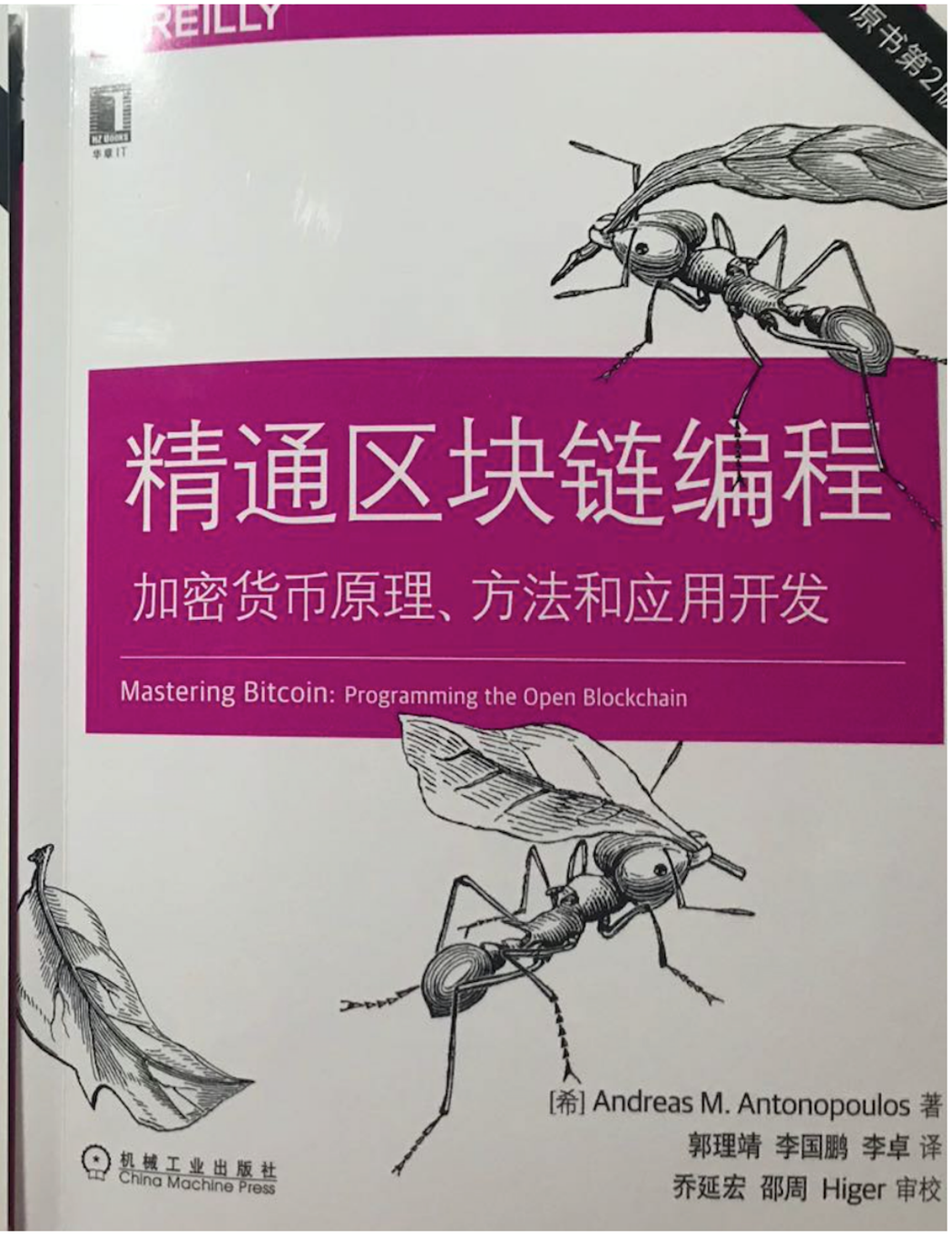

区块链定义与特性
会计视角
逻辑挑战
举例、面临挑战
数字货币
金融视角
区块链发展
1.0, 2.0, 3.0,
存证, DAPP
分布、集中、共识
网络视角
计算视角
基础设施、数字化

简介



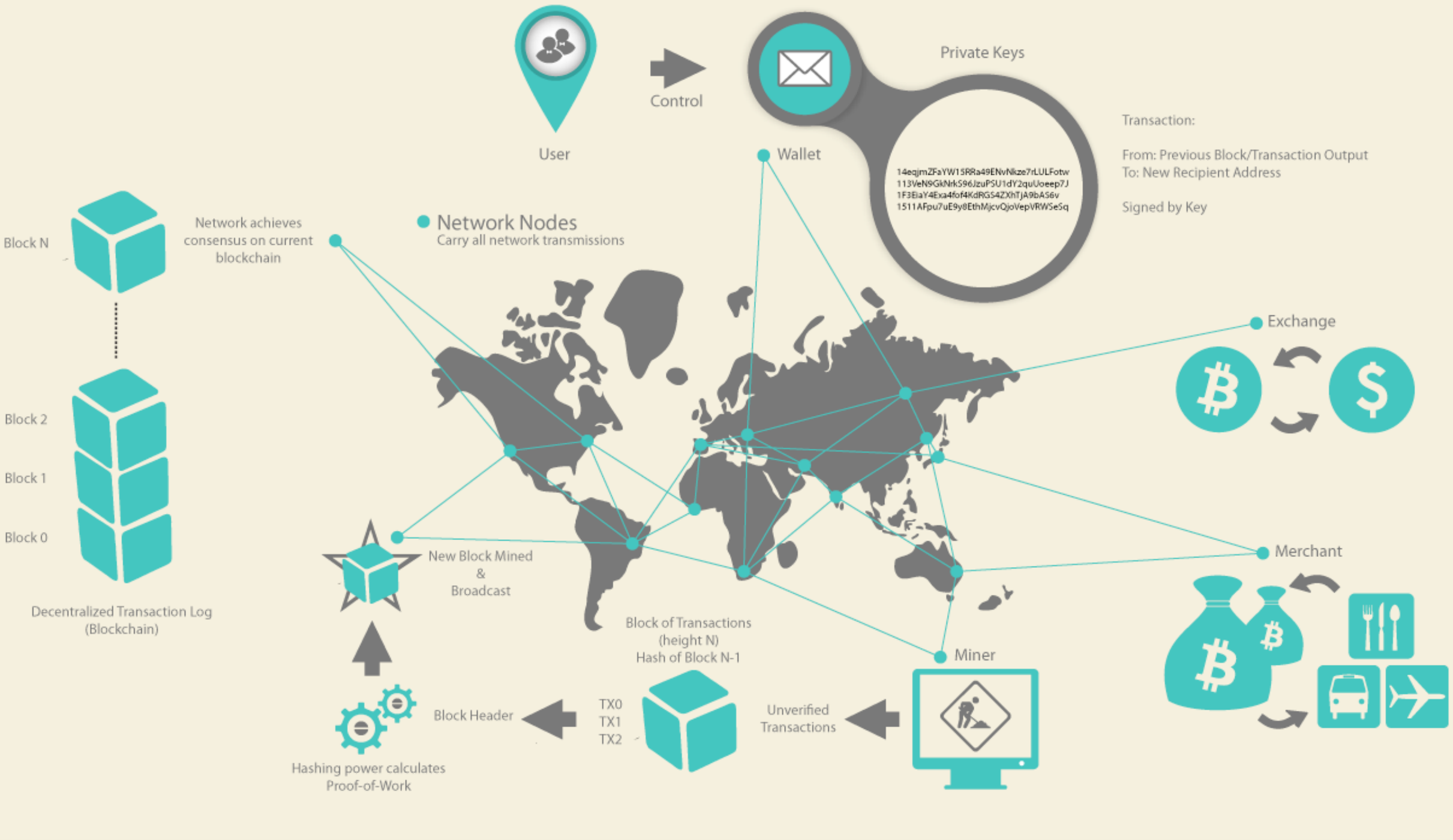
参考书


O'REILLY
第2版
Mastering
Bitcoin
精通比特币（影印版）
Andreas M. Antonopoulos 著
東南大學出版社


REILLY
精通区块链编程
加密货币原理、方法和应用开发
Mastering Bitcoin: Programming the Open Blockchain
[希] Andreas M. Antonopoulos 著
郭理靖 李国鹏 李卓 译
乔延宏 邵周 Higer 审校
机械工业出版社
China Machine Press

Mastering Bitcoin

Bitcoin如何工作



概念定义

构成数字货币生态系统基础概念和技术的总称

比特币网络中参与者存储和传输的货币单位

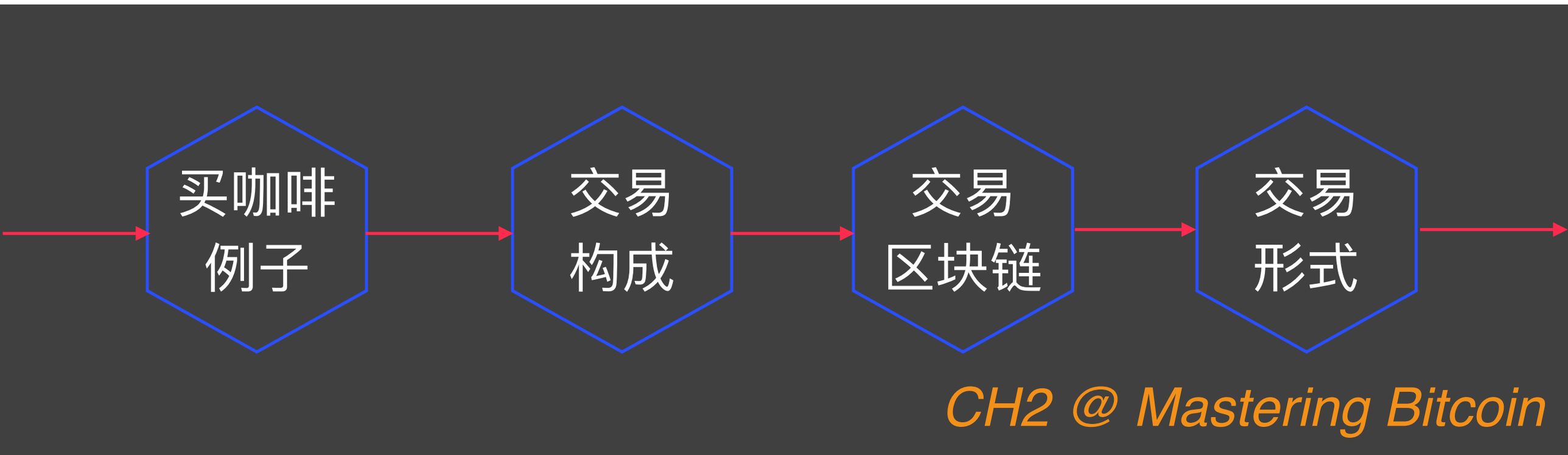
比特币是虚拟的，本身也不是简单数据化的

用户通过网络进行比特币进行转账和可以做到和传统货币一样的事情

比特币隐含在汇款方到收款方的转账交易中，用户用自己私钥来证明

传统银行依靠发行和结算，比特币依靠挖矿

基本原理



交易例子 – 买咖啡

```
bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA?
amount=0.015&
label=Bob%27s%20Cafe&
message=Purchase%20at%20Bob%27s%20Cafe
```

```
A bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"
The payment amount: "0.015"
A label for the recipient address: "Bob's Cafe"
A description for the payment: "Purchase at Bob's Cafe"
```

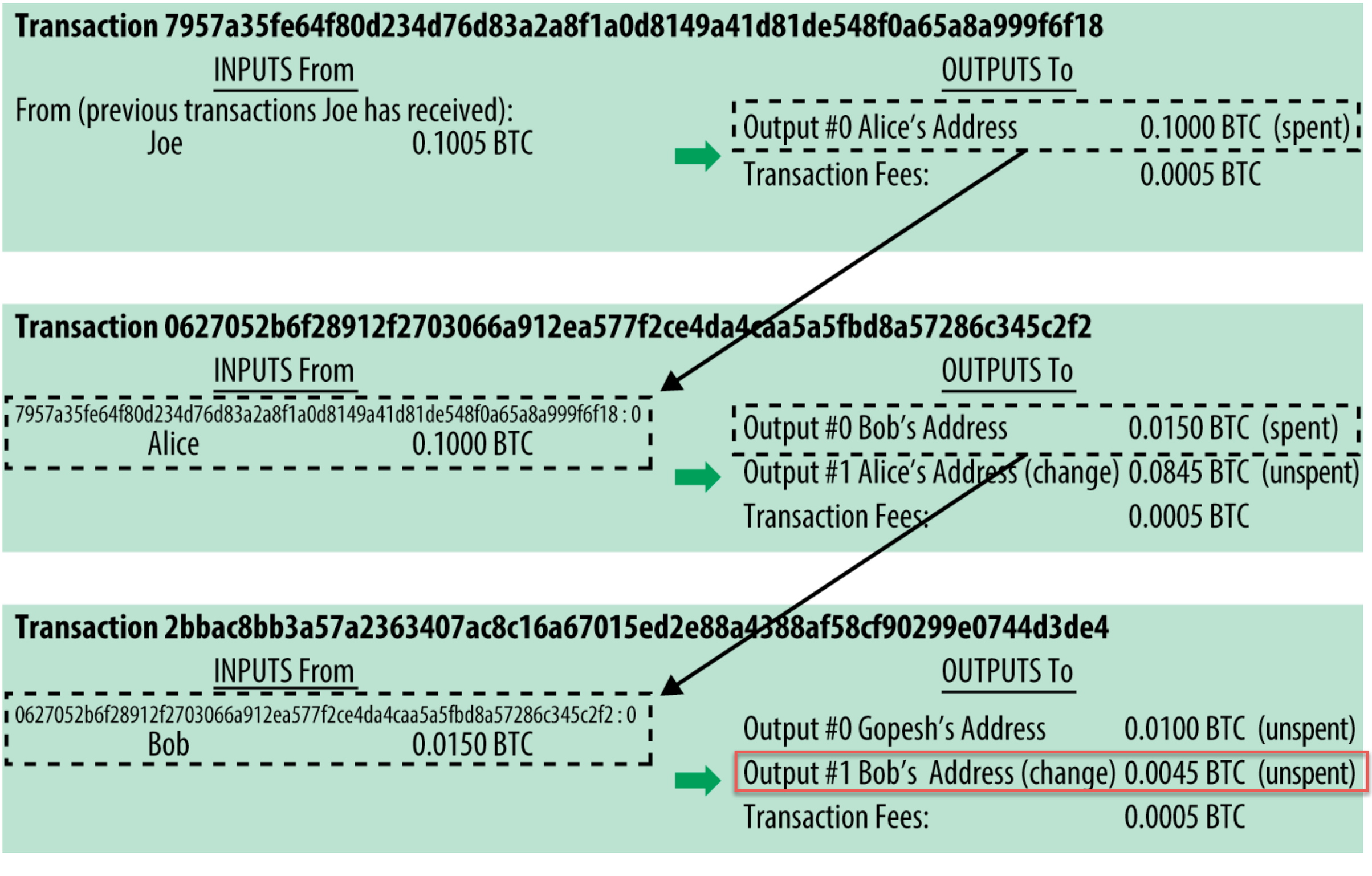
交易构成

Transaction as Double-Entry Bookkeeping

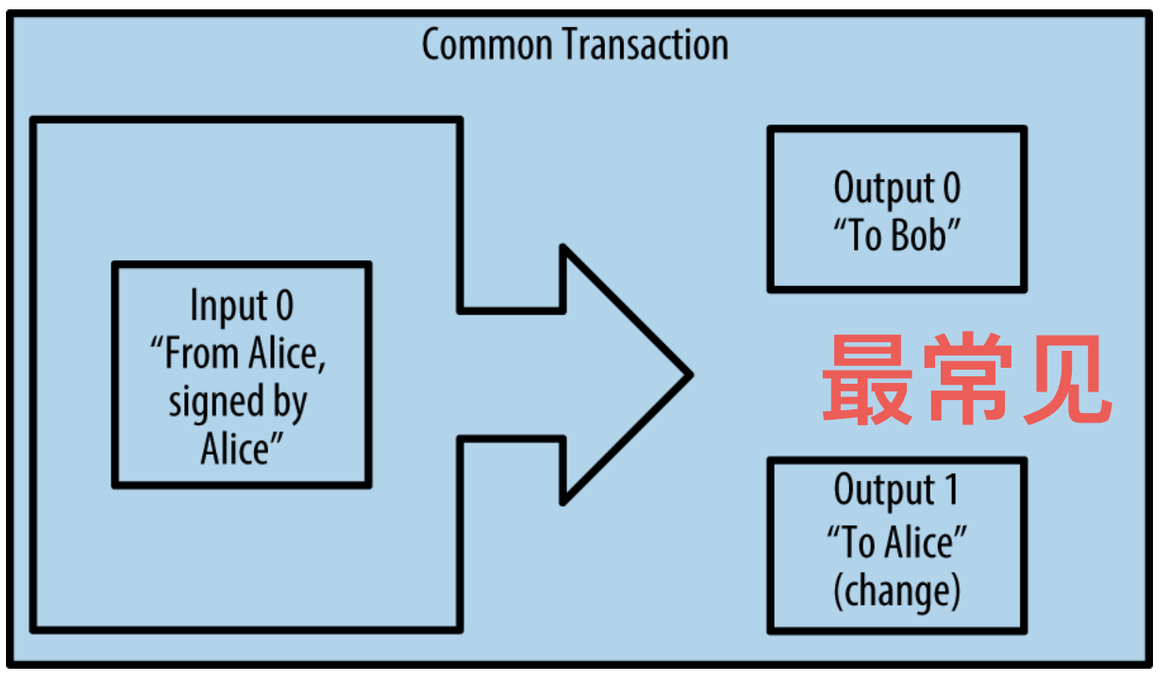
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

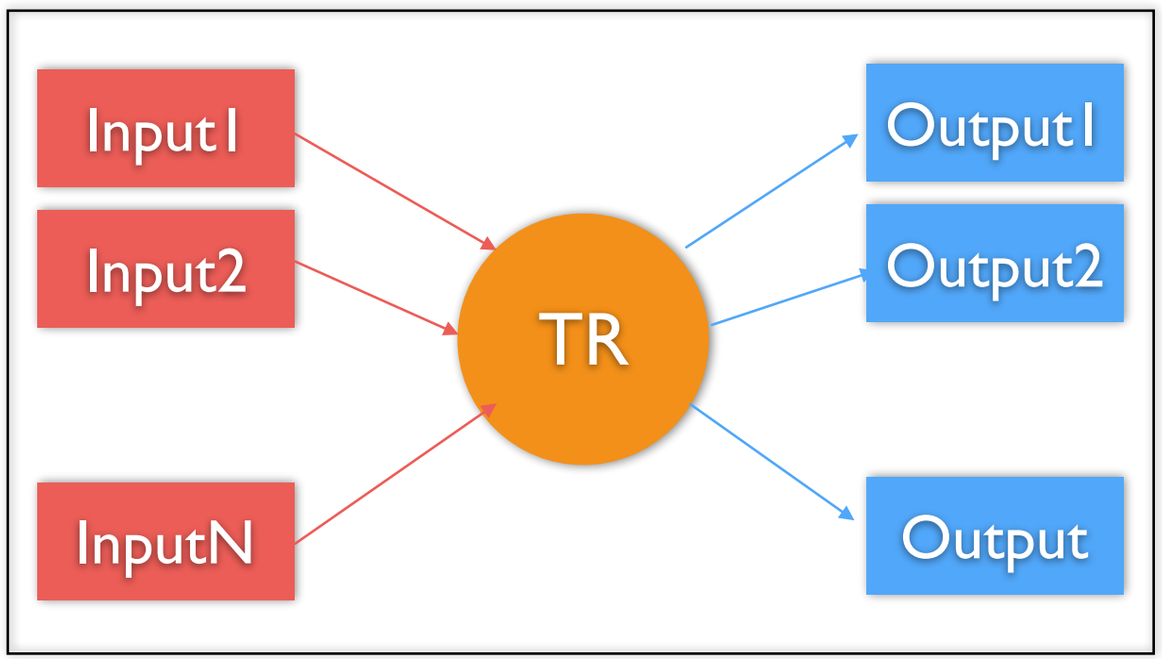
	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

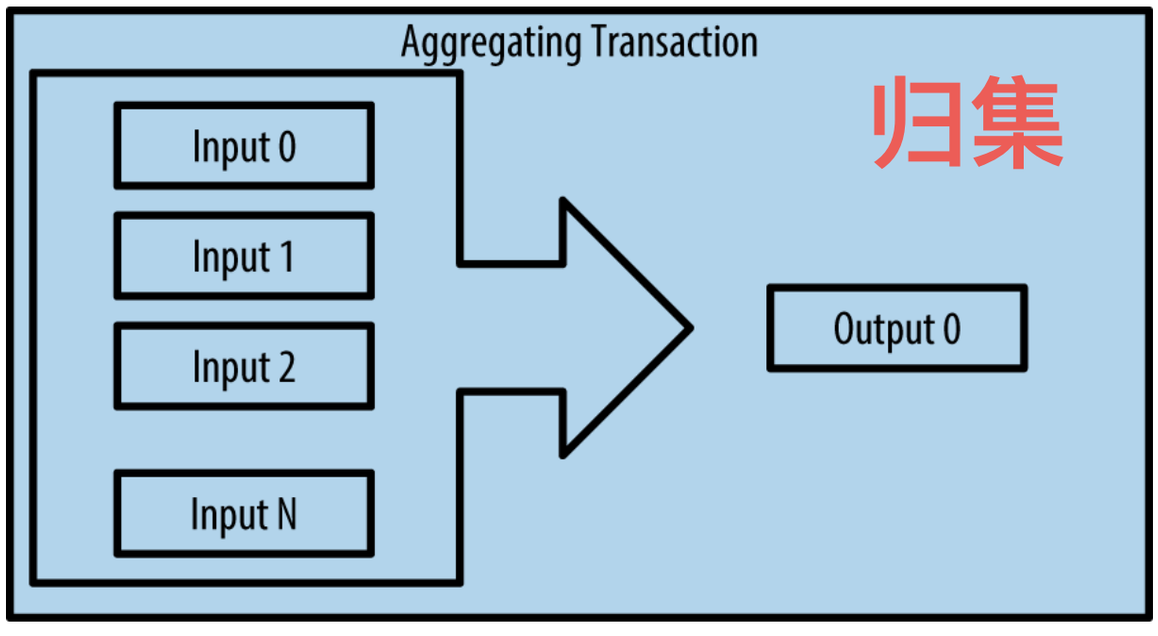
交易链

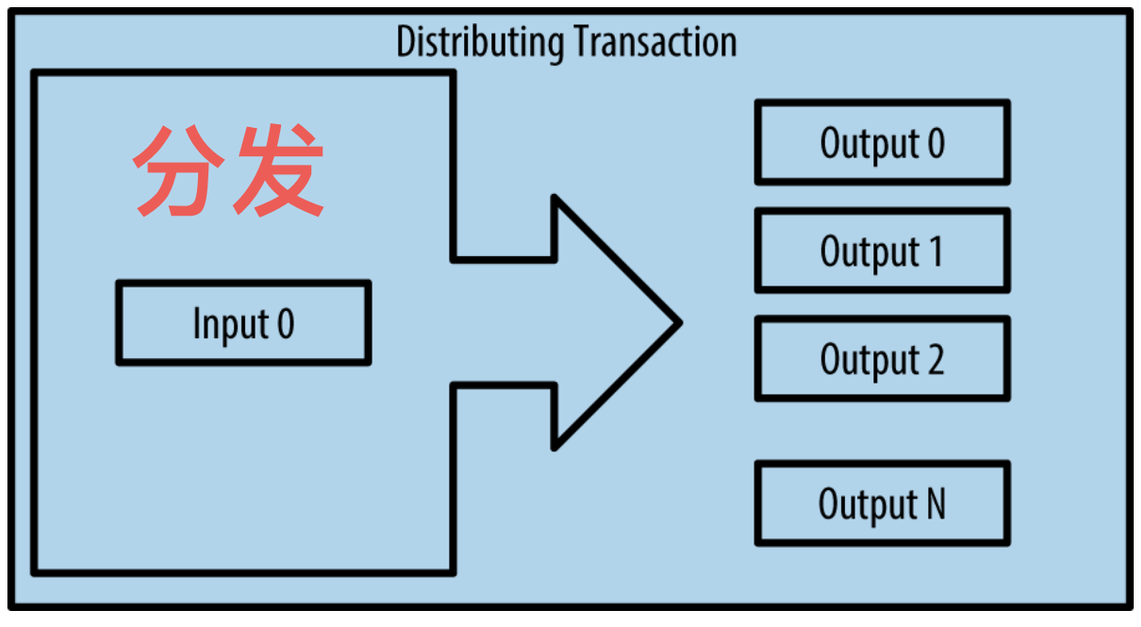

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18
INPUTS From
From (previous transactions Joe has received):
Joe 0.1005 BTC
OUTPUTS To
Output #0 Alice's Address 0.1000 BTC (spent)
Transaction Fees: 0.0005 BTC
Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2
INPUTS From
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18 : 0
Alice 0.1000 BTC
OUTPUTS To
Output #0 Bob's Address 0.0150 BTC (spent)
Output #1 Alice's Address (change) 0.0845 BTC (unspent)
Transaction Fees: 0.0005 BTC
Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4
INPUTS From
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2 : 0
Bob 0.0150 BTC
OUTPUTS To
Output #0 Gopesh's Address 0.0100 BTC (unspent)
Output #1 Bob's Address (change) 0.0045 BTC (unspent)
Transaction Fees: 0.0005 BTC

交易形式


Common Transaction
Input 0
"From Alice, signed by Alice"
Output 0
"To Bob"
最常见
Output 1
"To Alice" (change)


Input1
Input2
InputN
TR
Output1
Output2
Output


Aggregating Transaction
归集
Input 0
Input 1
Input 2
Input N
Output 0


Distributing Transaction
分发
Input 0
Output 0
Output 1
Output 2
Output N

交易描述

区块链浏览器

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

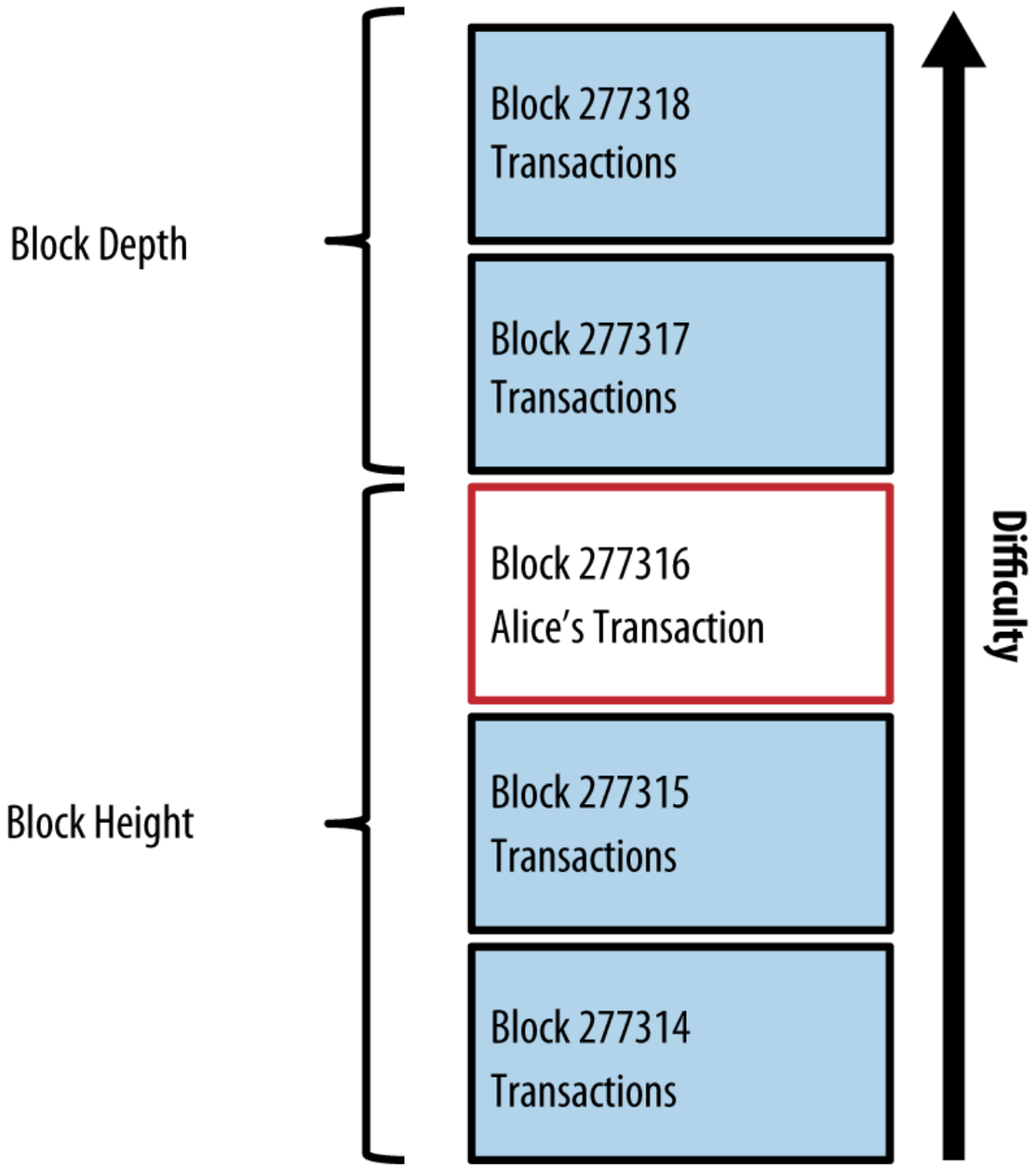
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

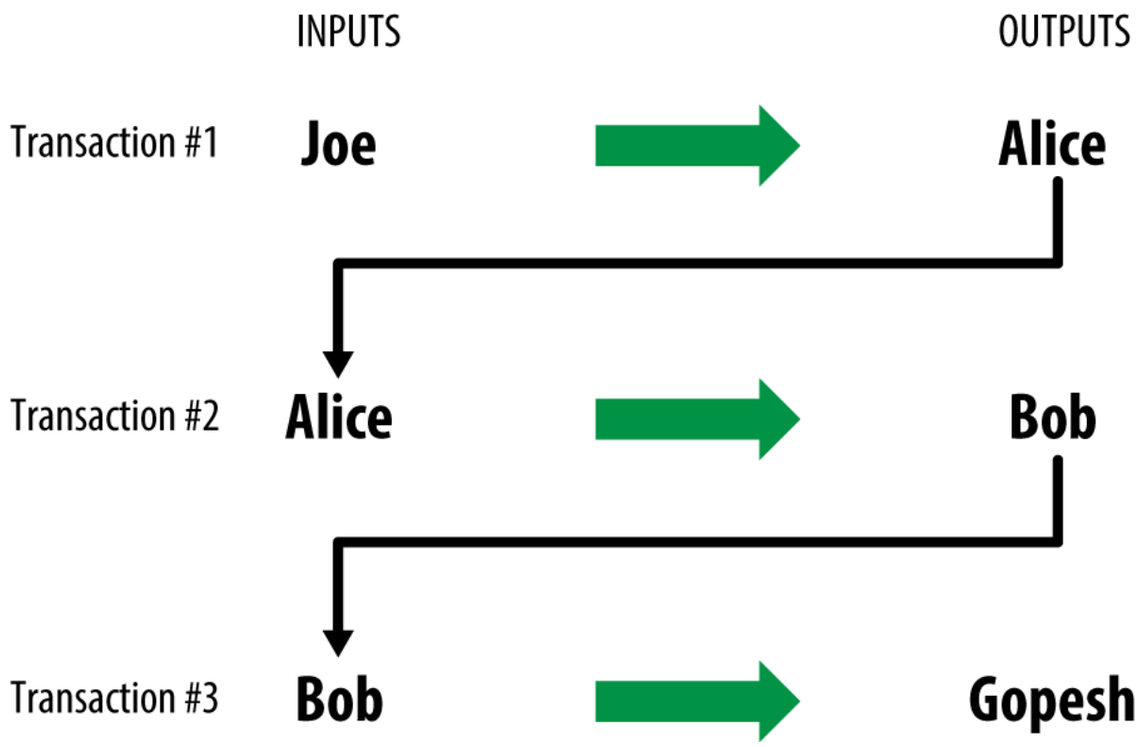
97 Confirmations | 0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

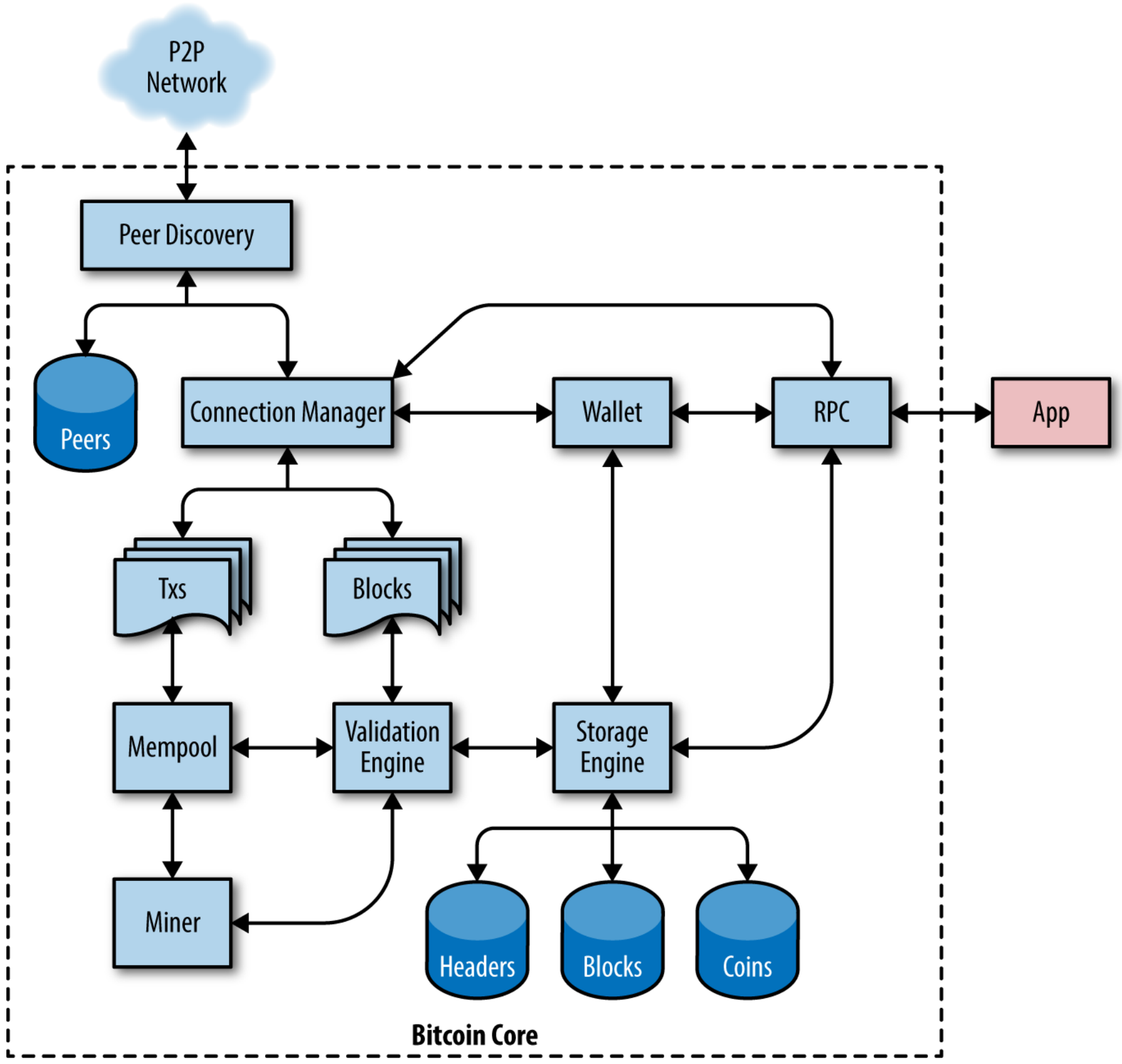
区块和链条


Block Depth
Block 277318
Transactions
Block 277317
Transactions
Block 277316
Alice's Transaction
Block 277315
Transactions
Block 277314
Transactions
Block Height
Difficulty

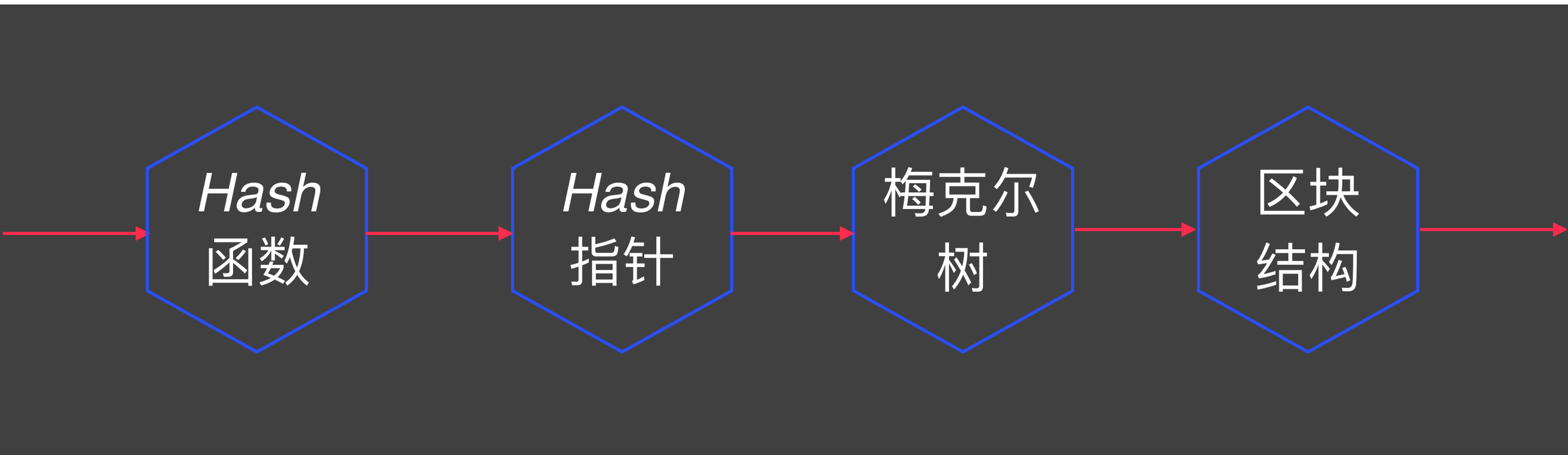

INPUTS
OUTPUTS
Transaction #1
Joe
Alice
Transaction #2
Alice
Bob
Transaction #3
Bob
Gopesh

核心客户端

Bitcoin核心架构



区块

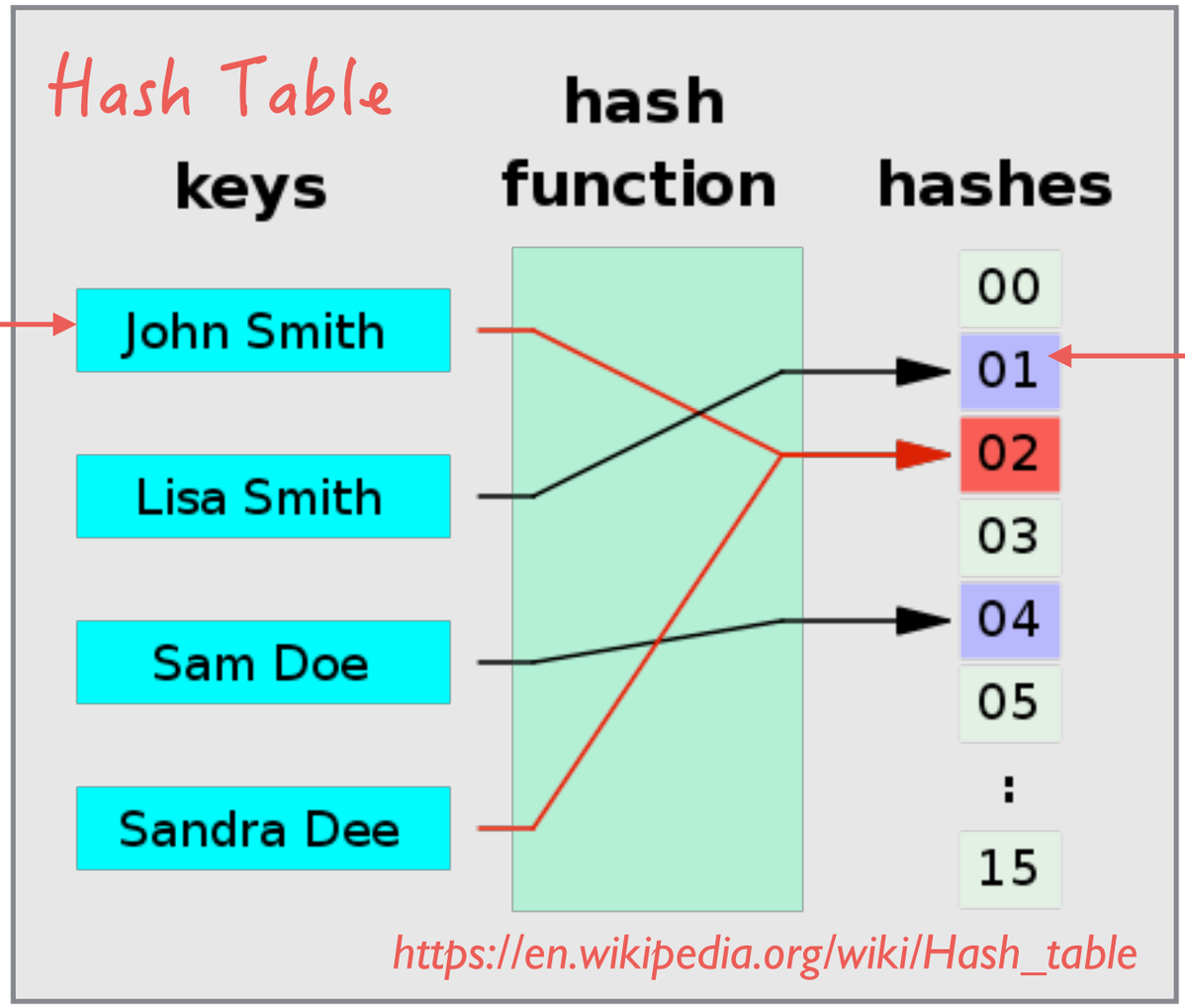


Hash函数

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

输入为任意大小的字符串

可以进行有效计算：例如O(n)



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

输出为固定大小，例如256位

同样的输入产生同样的输出

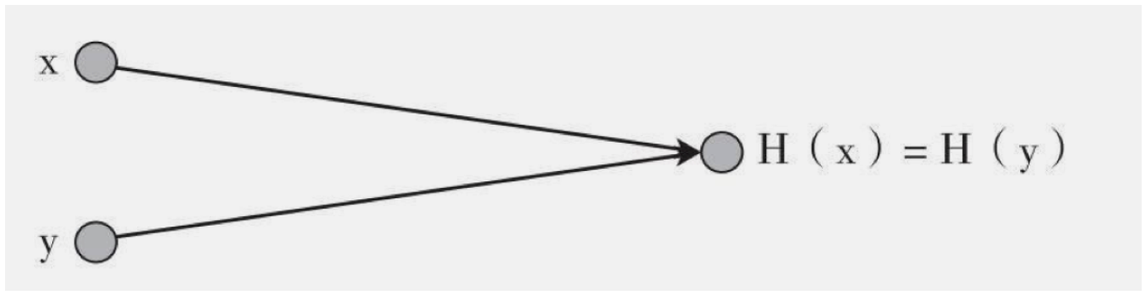
MEM2018 → SHA256 → 547d71f91fec62c23dee84cf2a5dcfd4bdc46a05b2ddd3253555c1b76be433e5

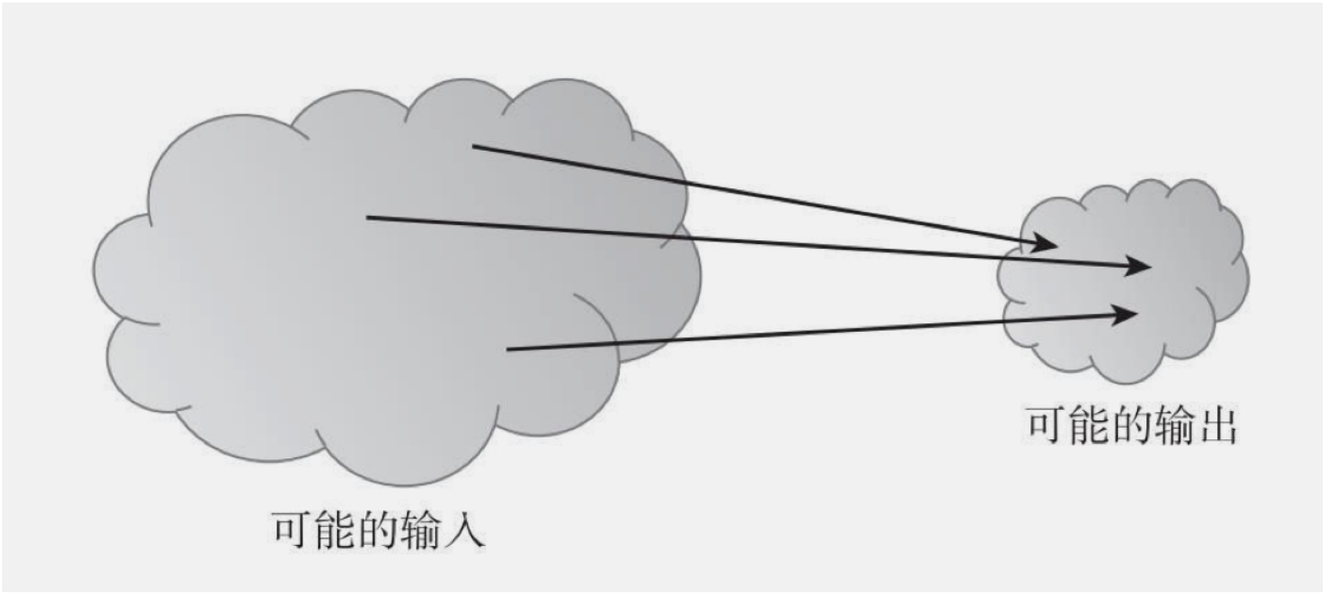
单向性

http://www.fileformat.info/tool/hash.htm

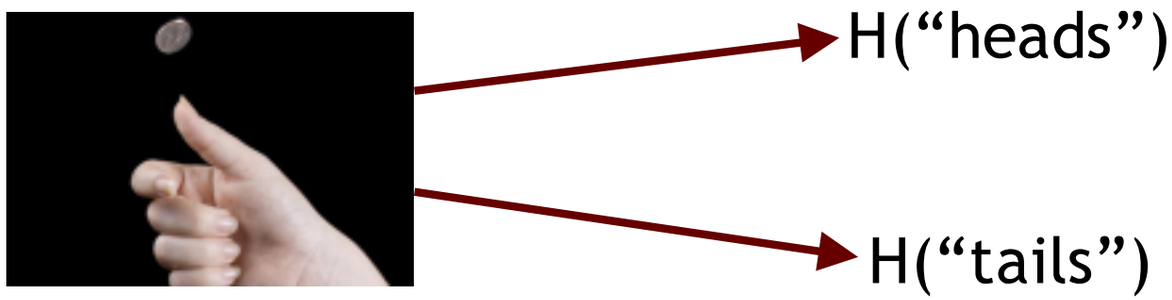
Hash函数

抗碰撞





隐匿性



给出$H(x)$，不能找到x

单向性

已知x，计算$H(x)$容易

已知$H(x)$，求x困难

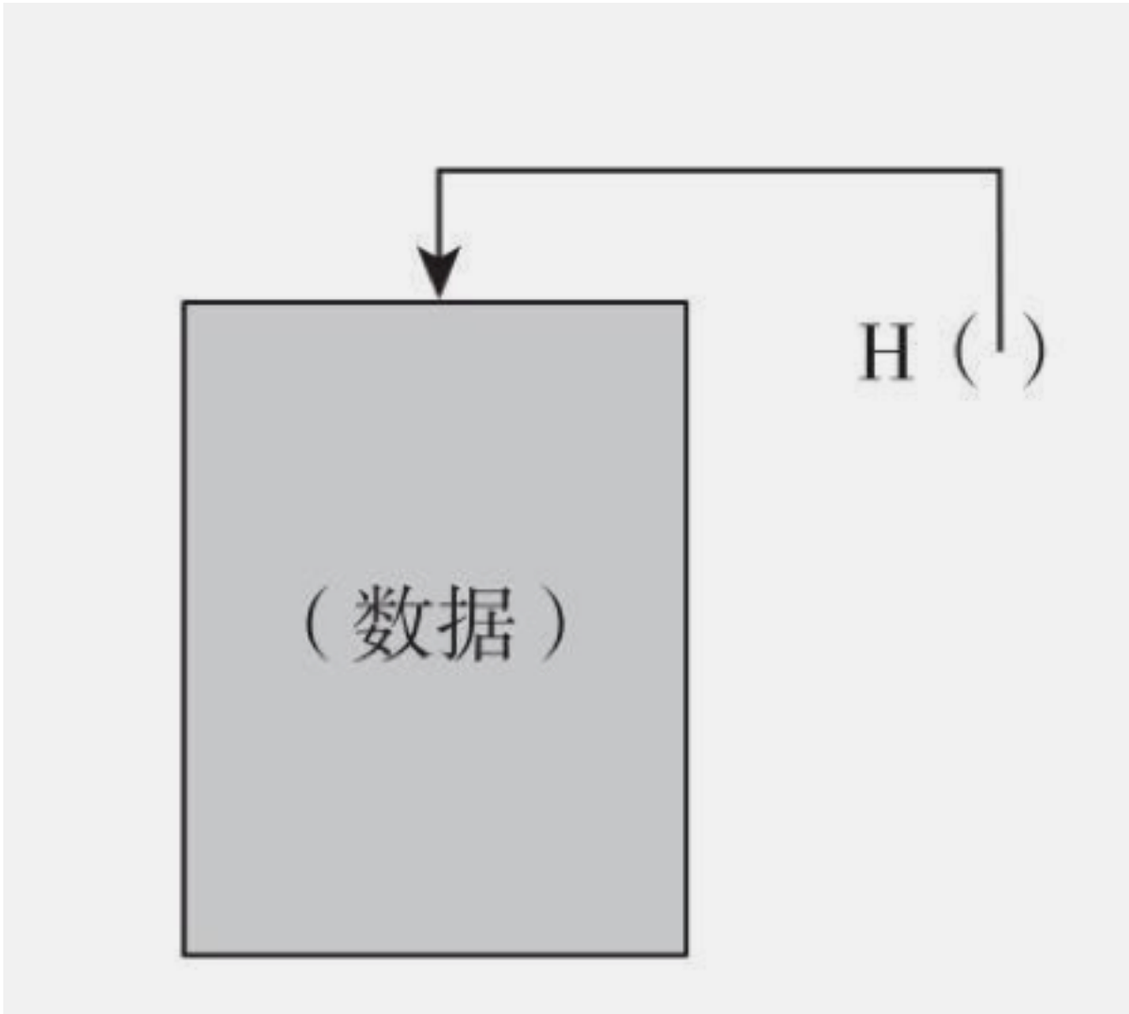
难题友好

Hash指针

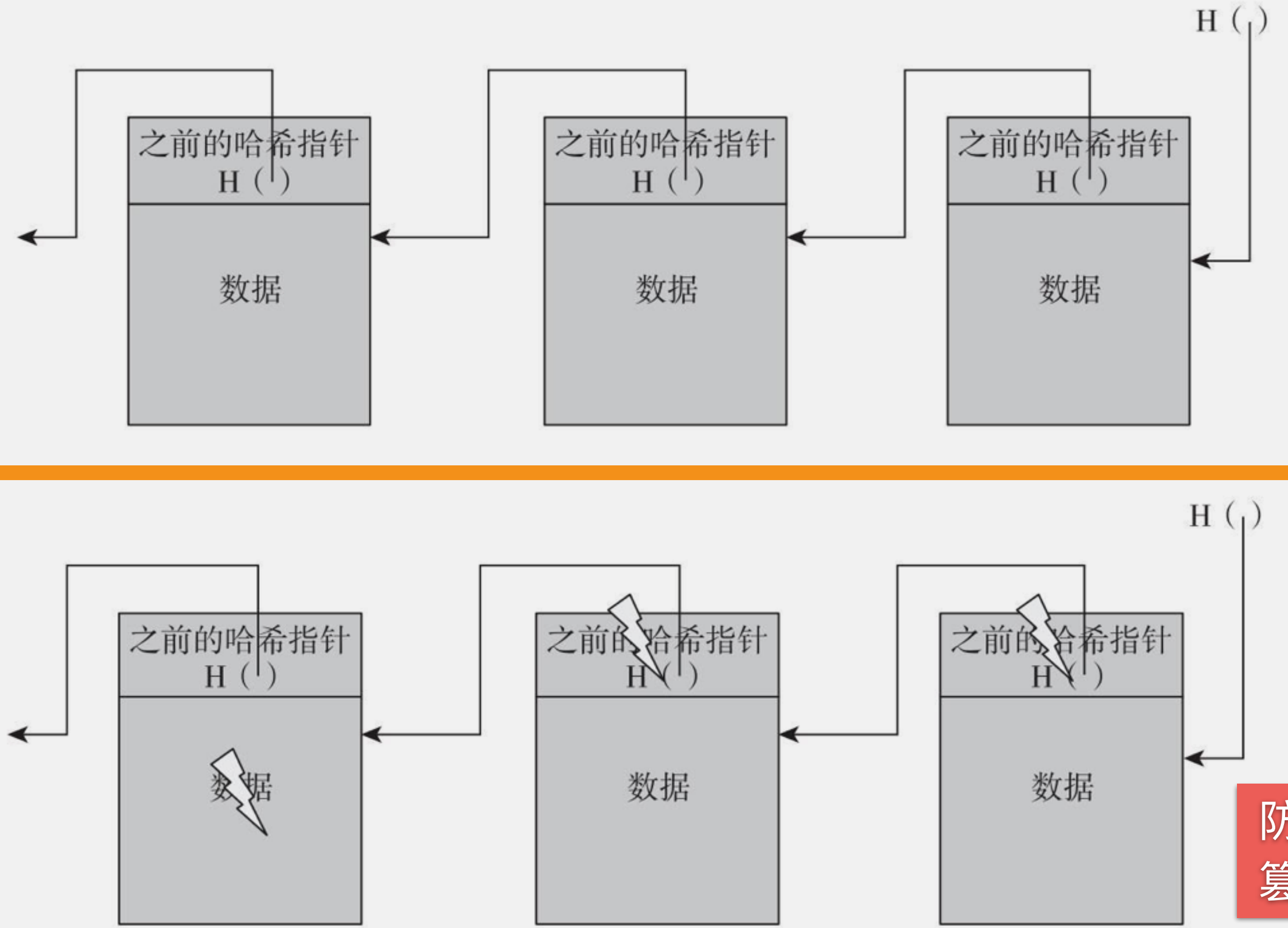
Hash指针：
是一个指向存储数据
及其数据Hash的指针

取回数据
验证数据是否改变

区块链的关键思想

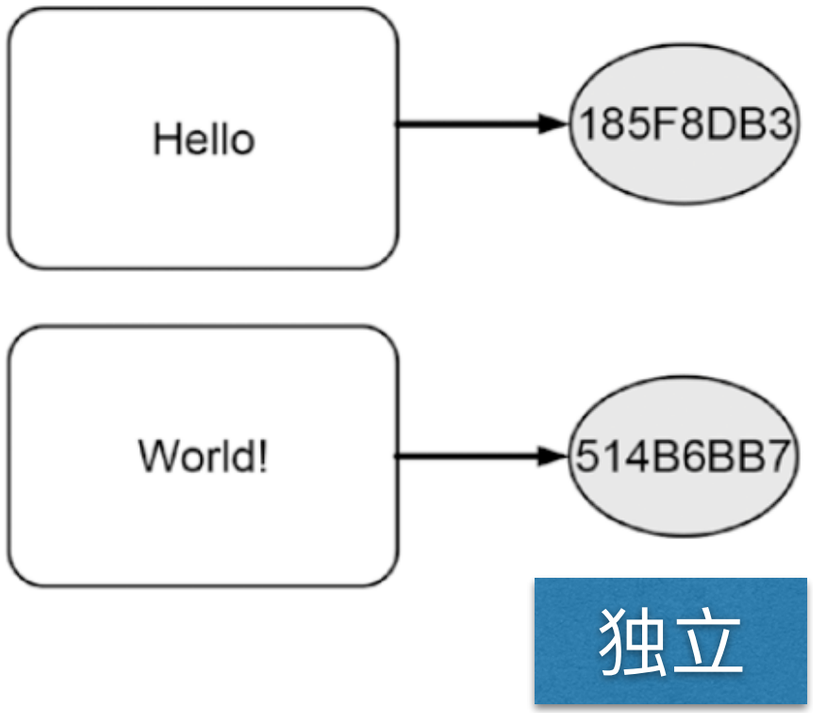


区块链

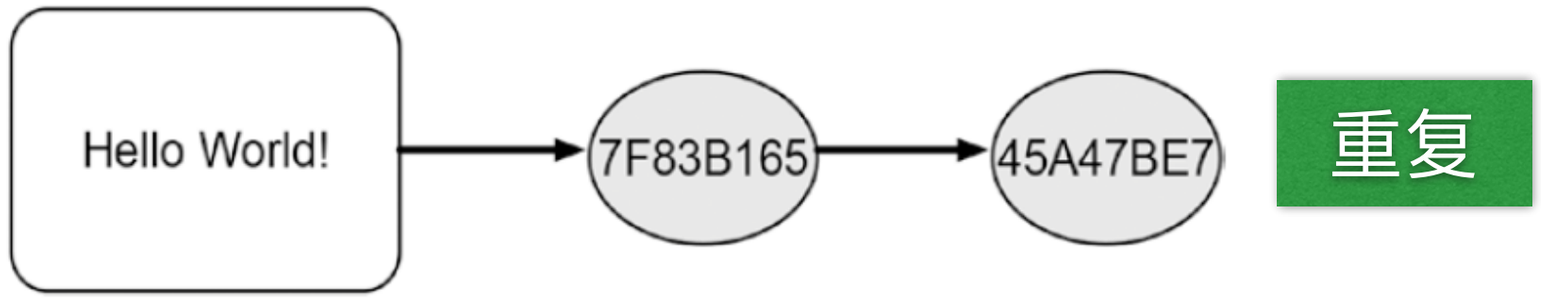

H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
防止
篡改

Hash数据模式

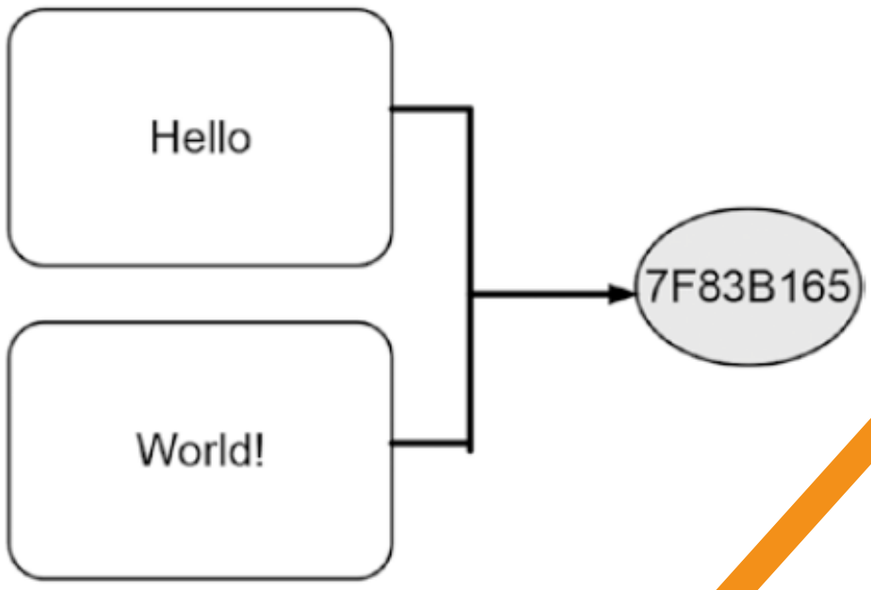
Blockchain Basics:A Non-Technical Introduction in 25 Steps @ APRESS



独立

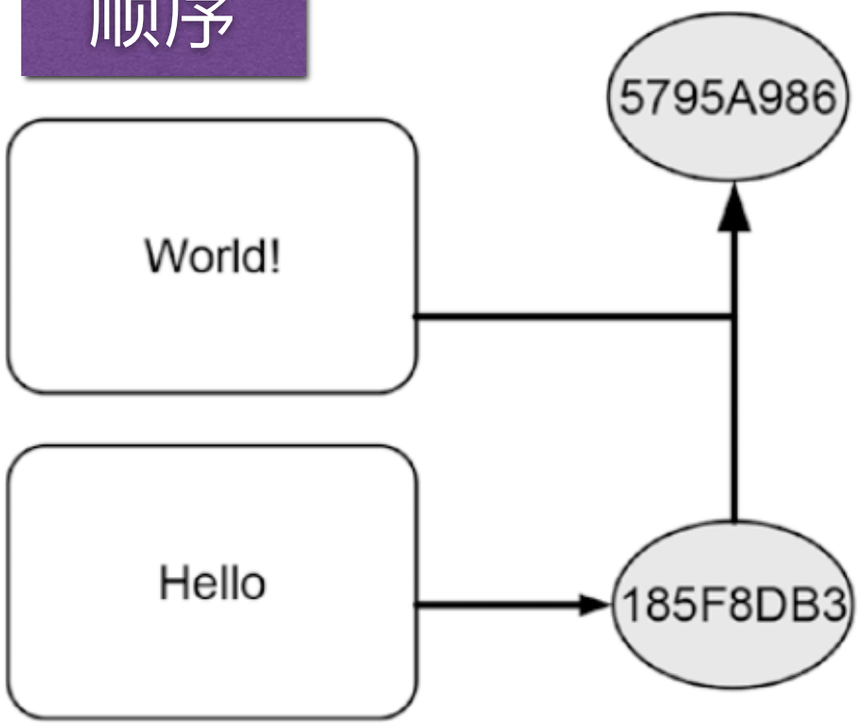


重复

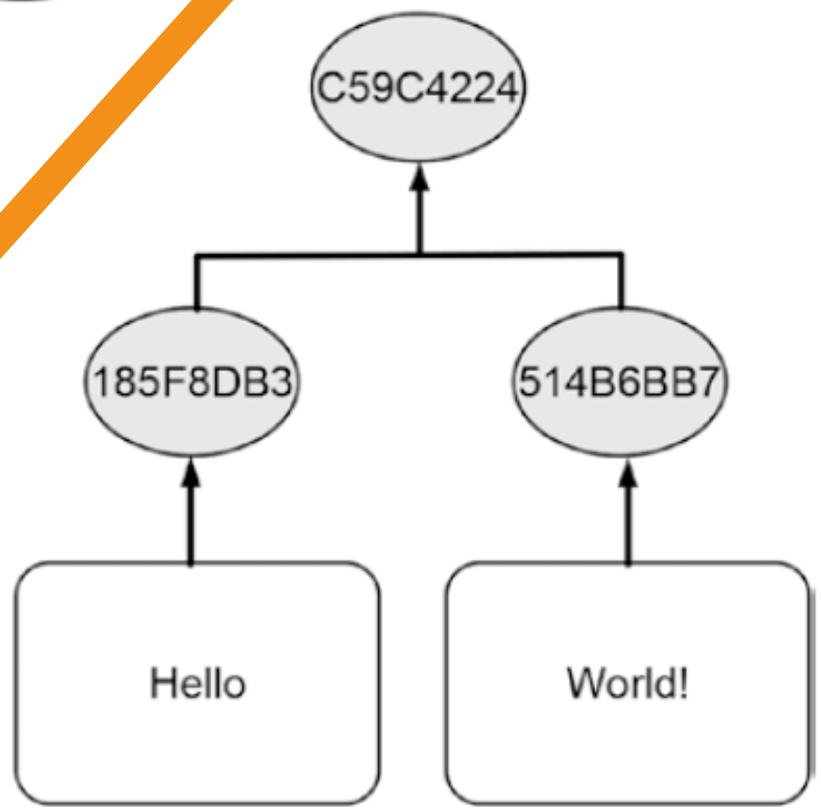


联合

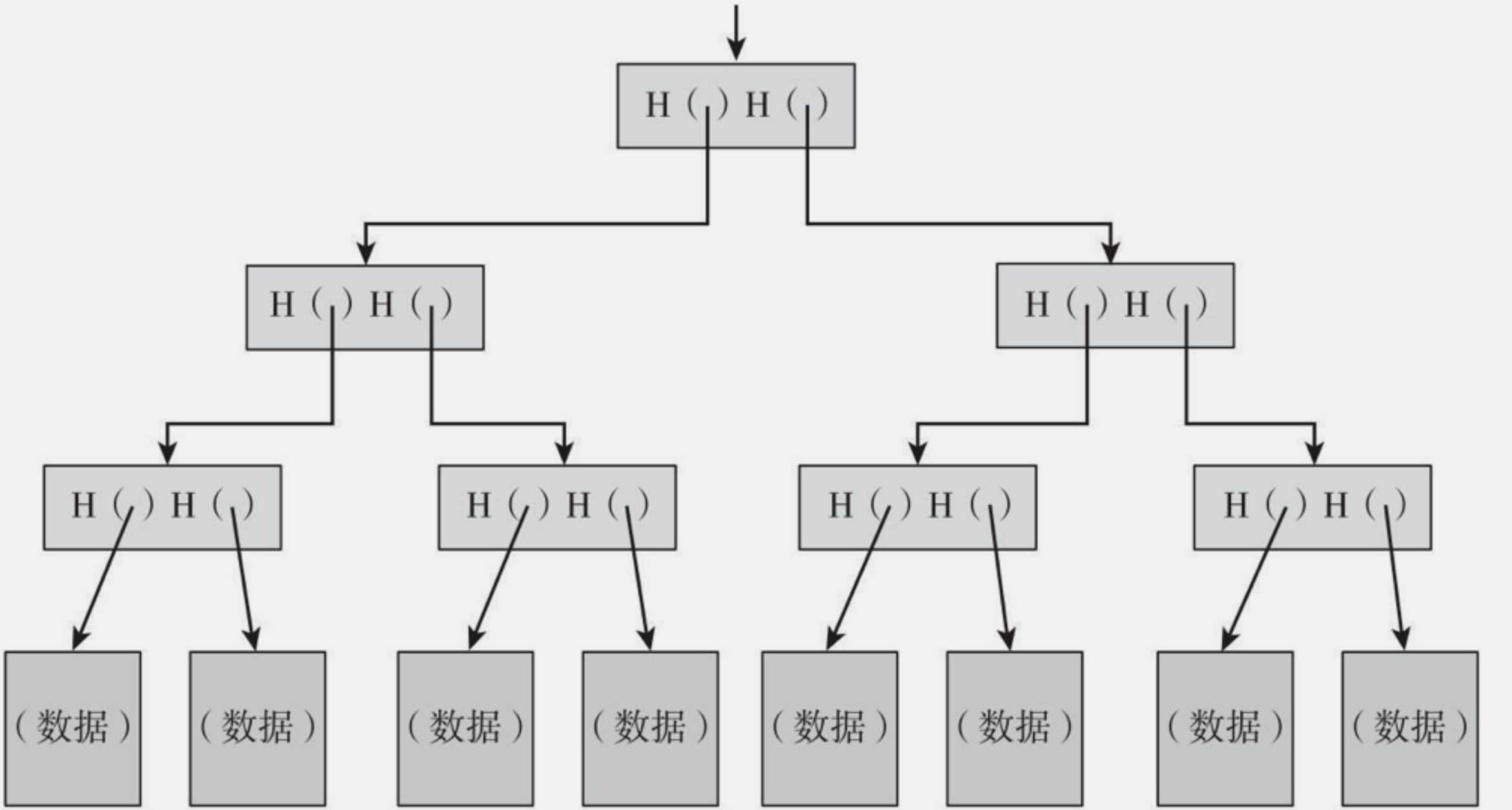
顺序



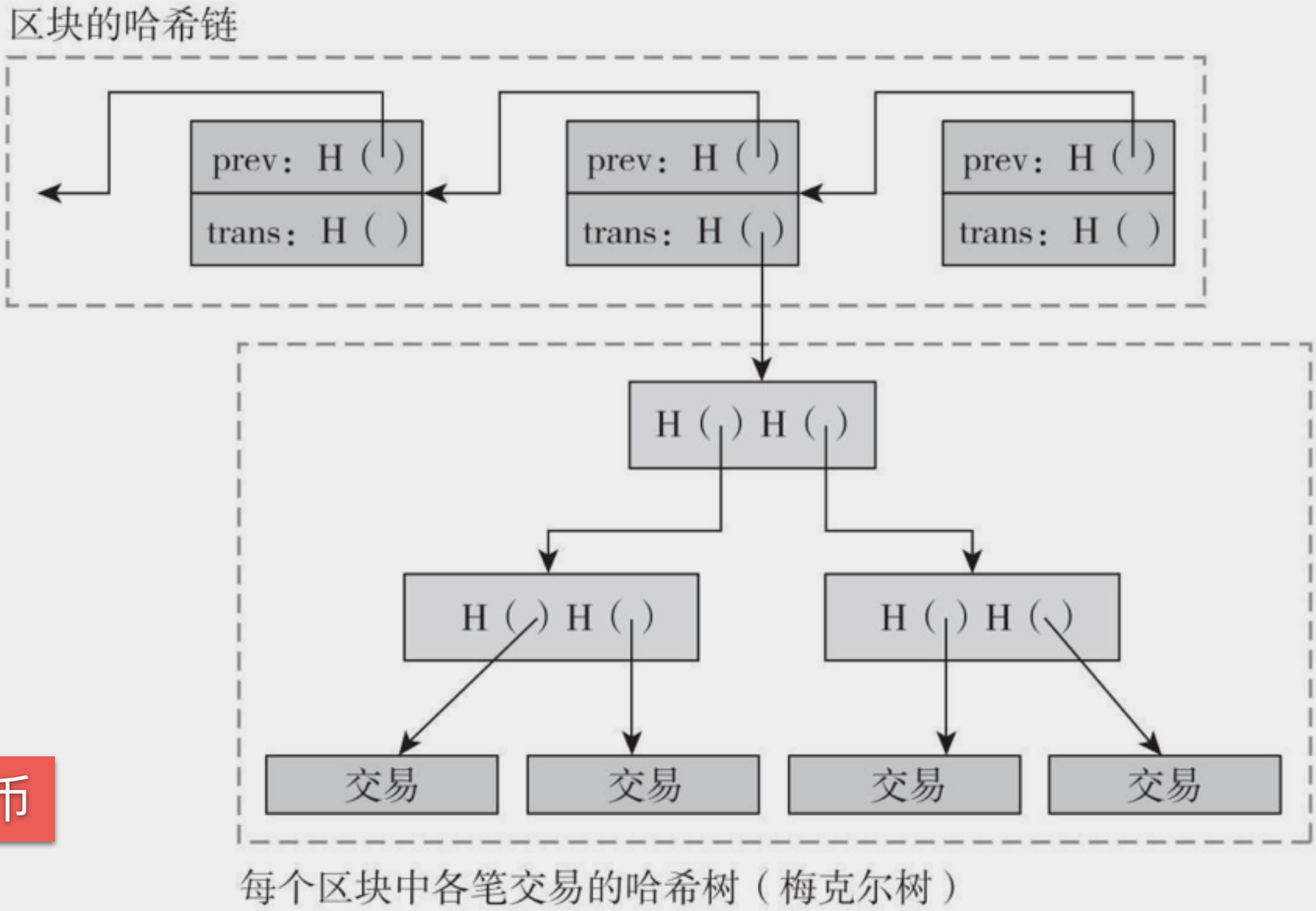
层次



梅克尔树



区块结构

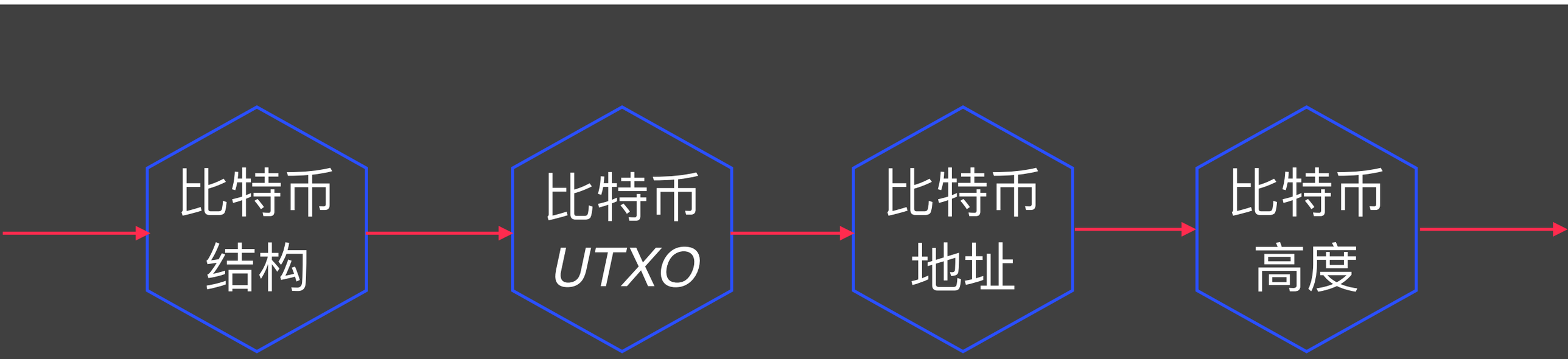


比特币

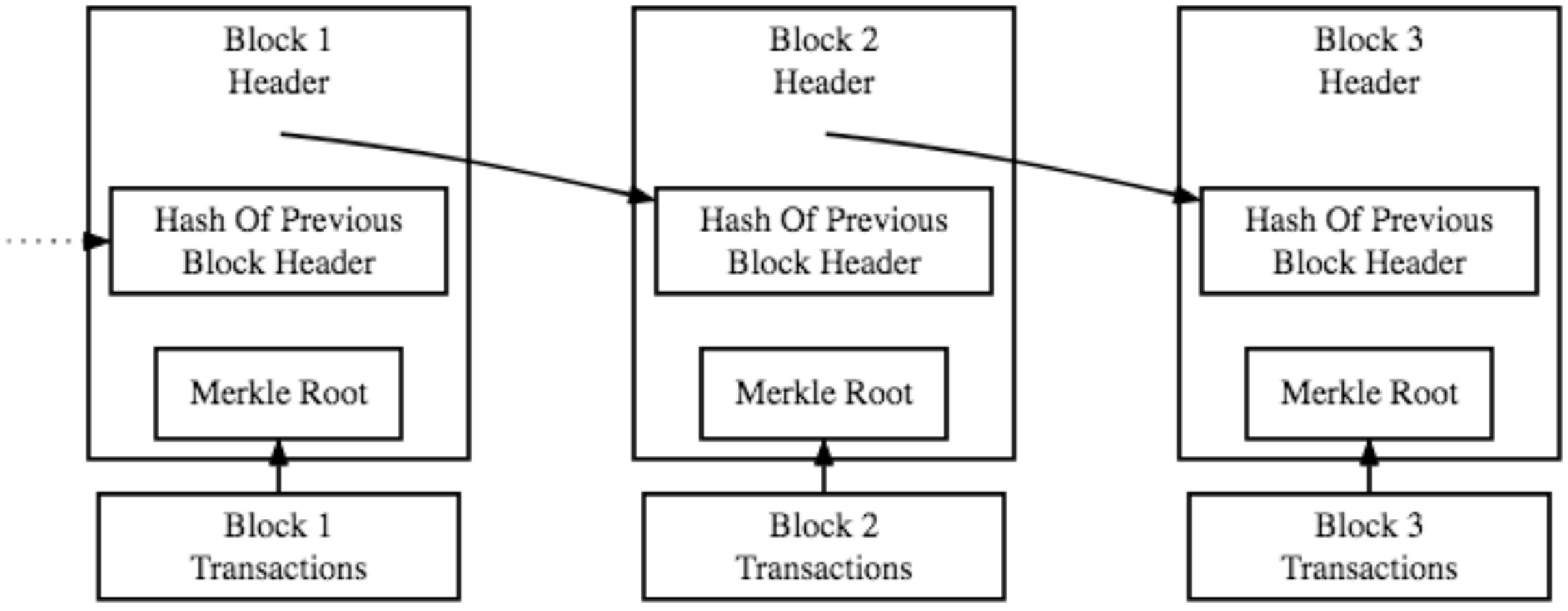
图3.7 比特币的区块链有两个哈希结构

注：一个就是把区块联结在一起的哈希链，另一个就是区块内部的交易哈希值梅克尔树。

比特币结构



比特币结构



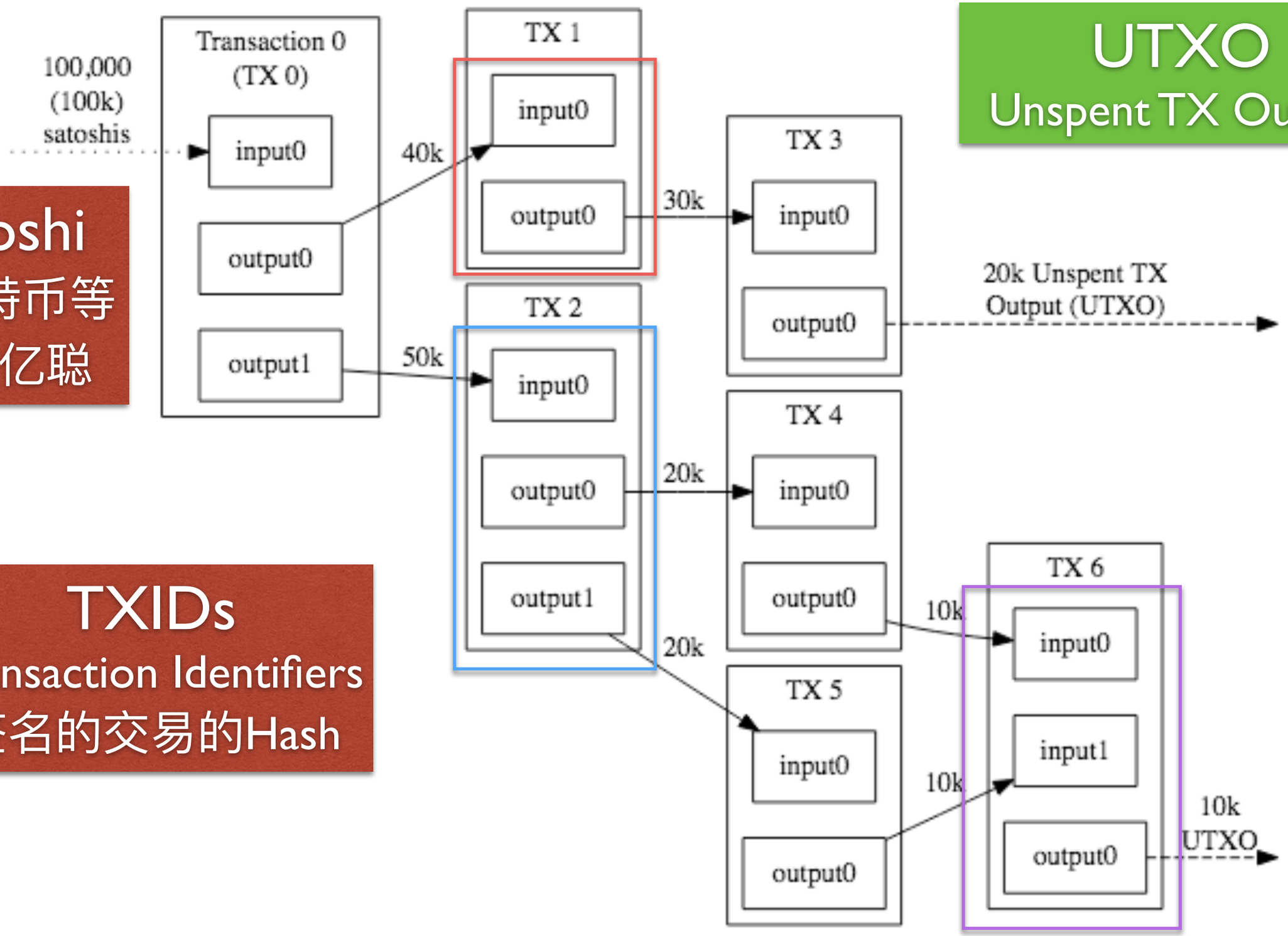
Simplified Bitcoin Block Chain

比特币UTXO

satoshi
一比特币等于一亿聪

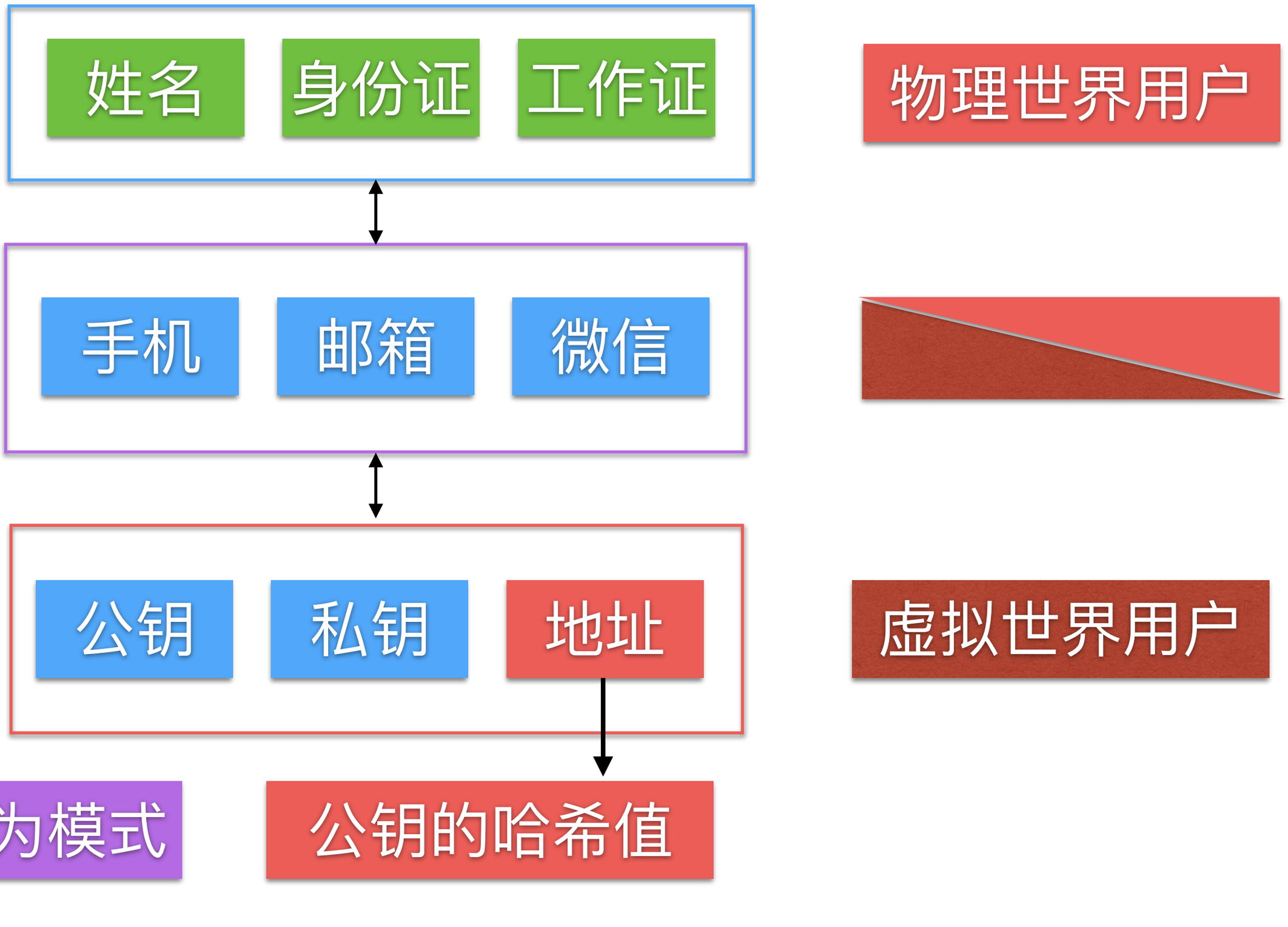
TXIDs
Transaction Identifiers
签名的交易的Hash

UTXO
Unspent TX Output

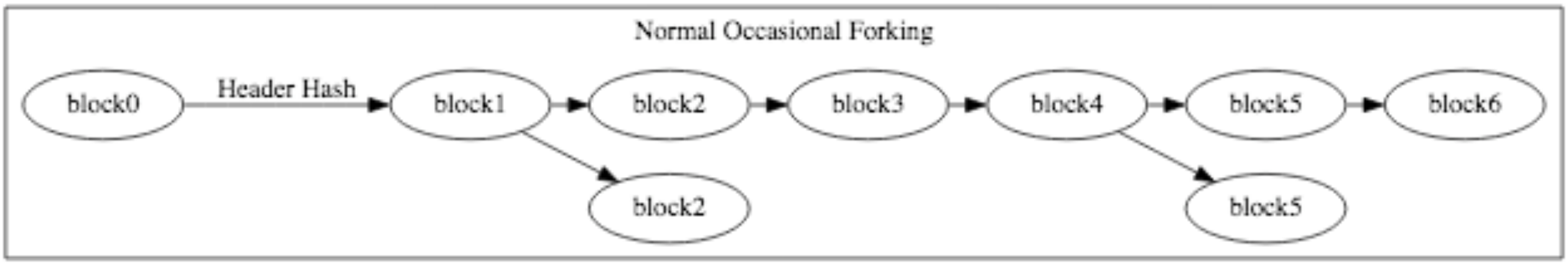


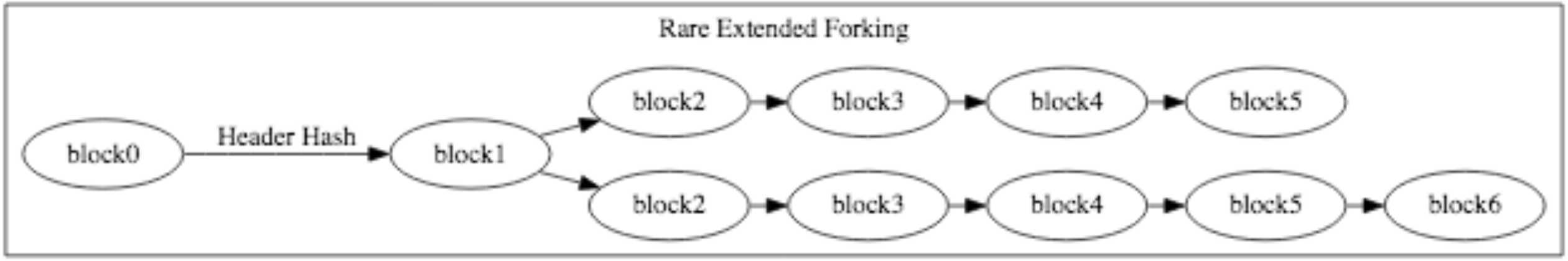
Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

比特币地址



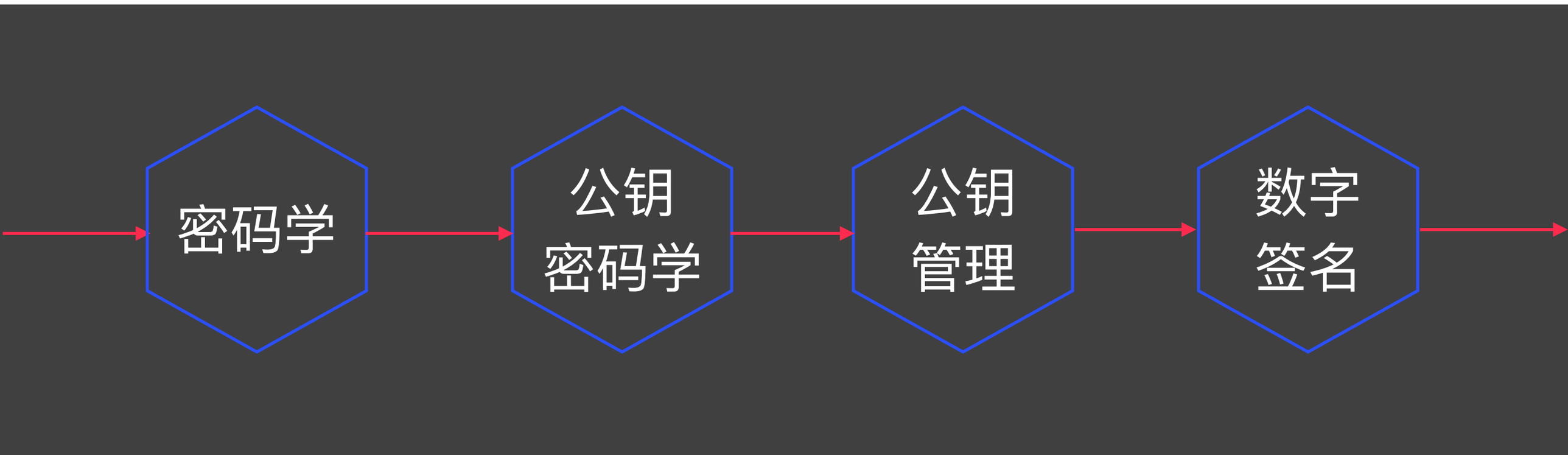
比特币高度





比特币高度　　比特币分叉

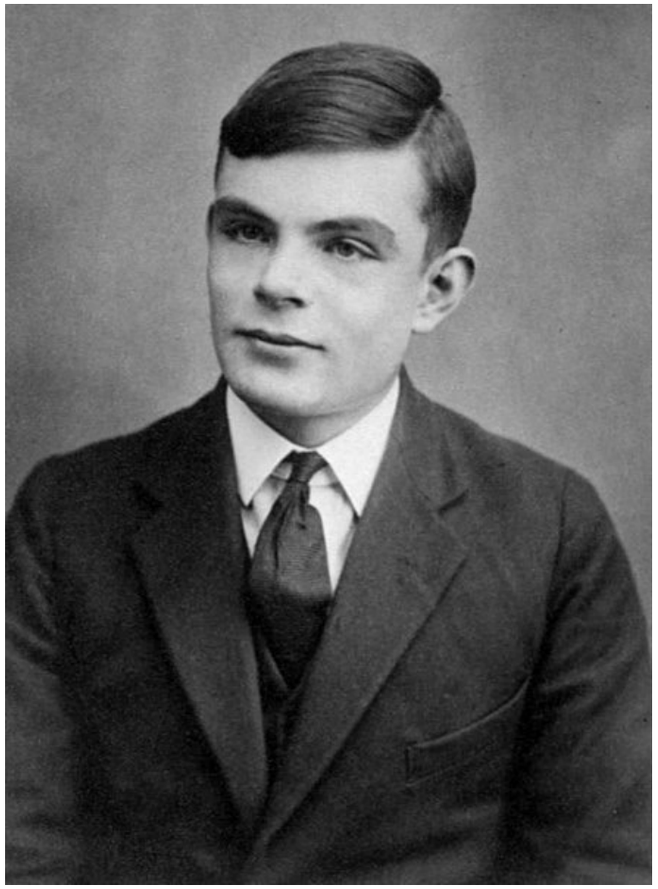
密码



密码学

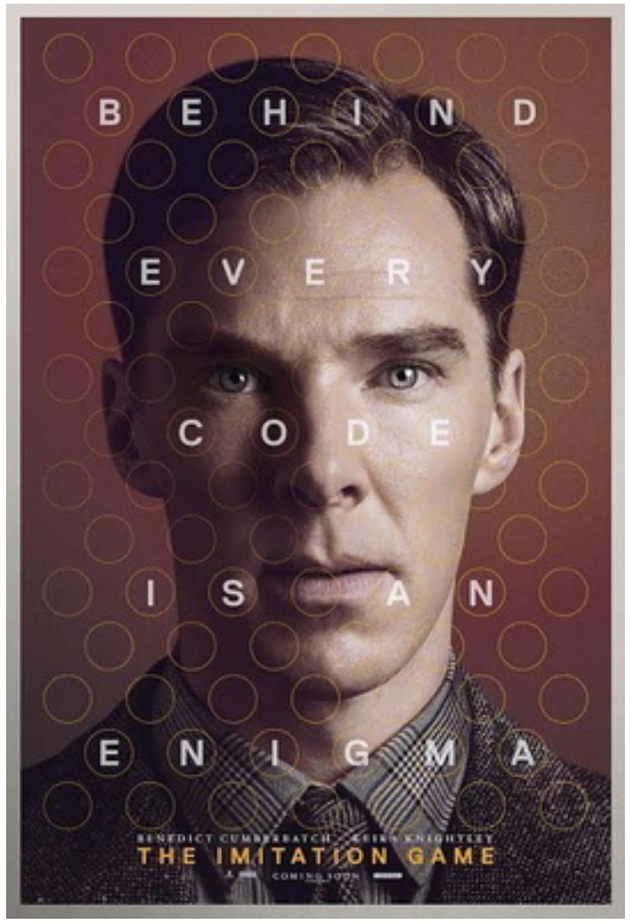
https://en.wikipedia.org/wiki/Alan_Turing

图灵

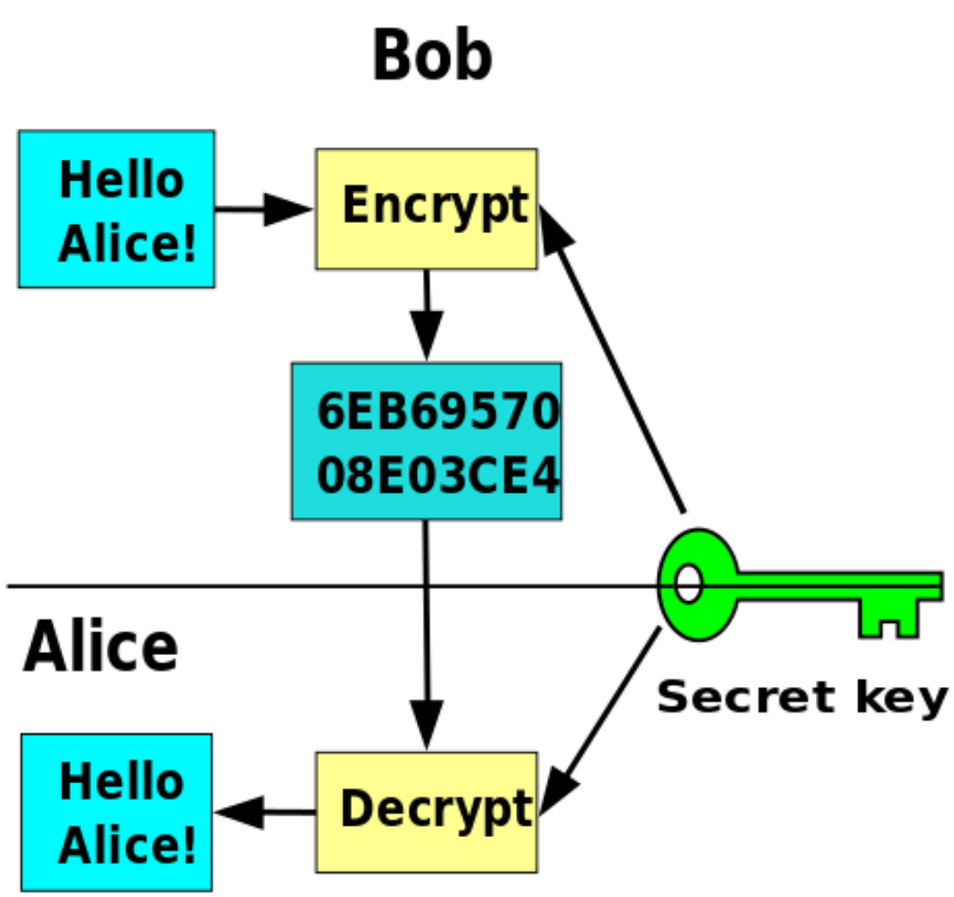


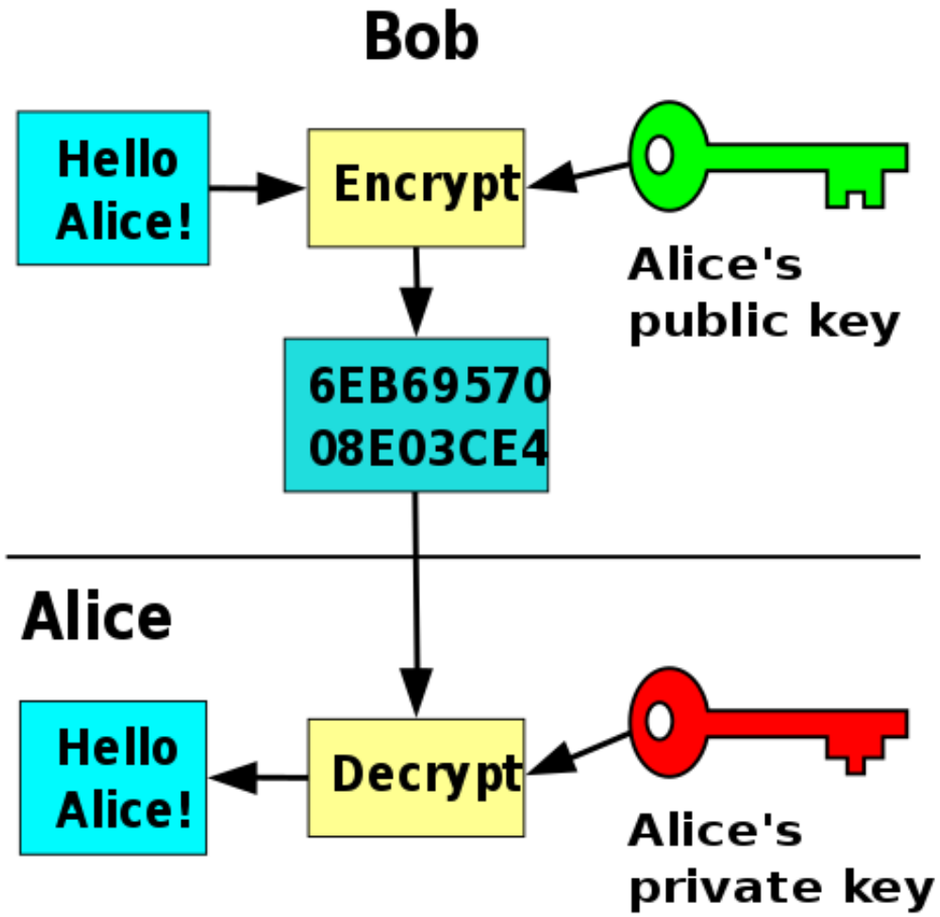
恩尼格玛密码机

模仿游戏



对称密码学 vs. 非对称密码学





对称密码学

封闭

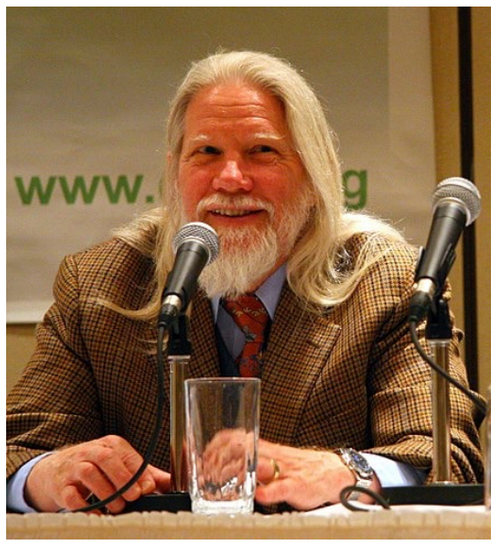
开放

非对称密码学

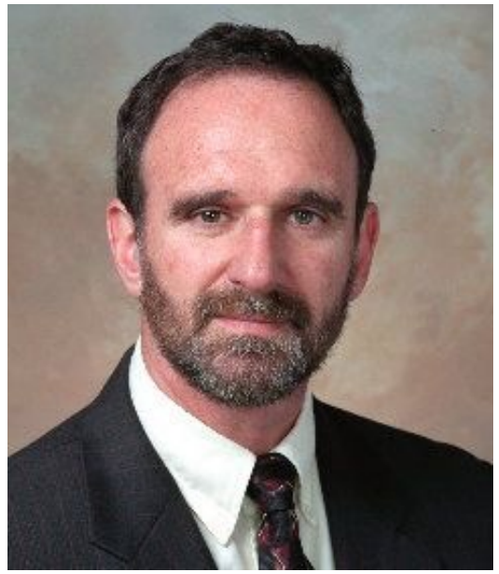
DH vs. RSA

2015年
图灵奖

1976



Whitfield Diffie



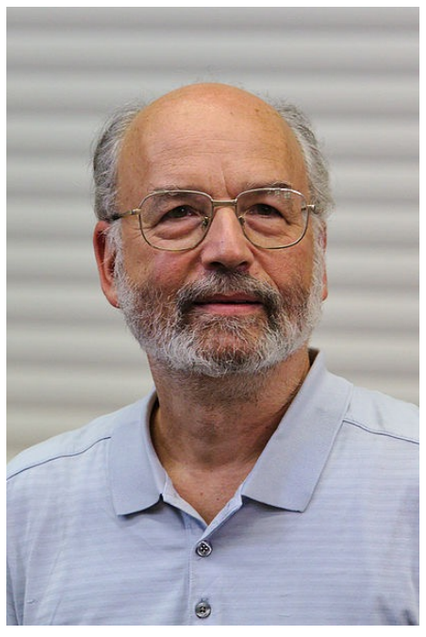
Martin Hellman

Ralph Merkle

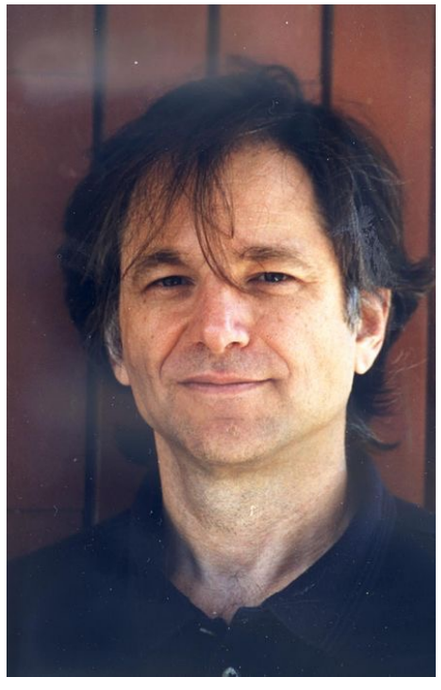
1978

2002年
图灵奖

Ronald L. Rivest



Adi Shamir



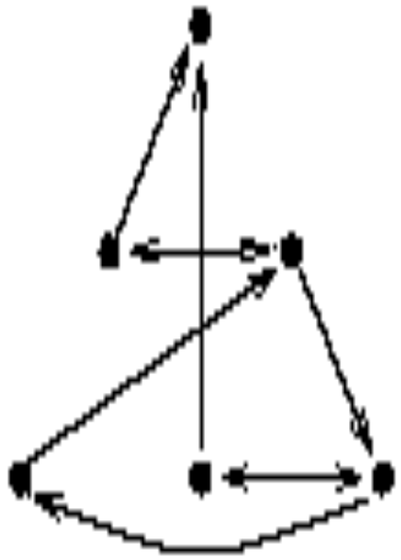
Leonard Max Adleman

公钥管理: PKI vs. PGP

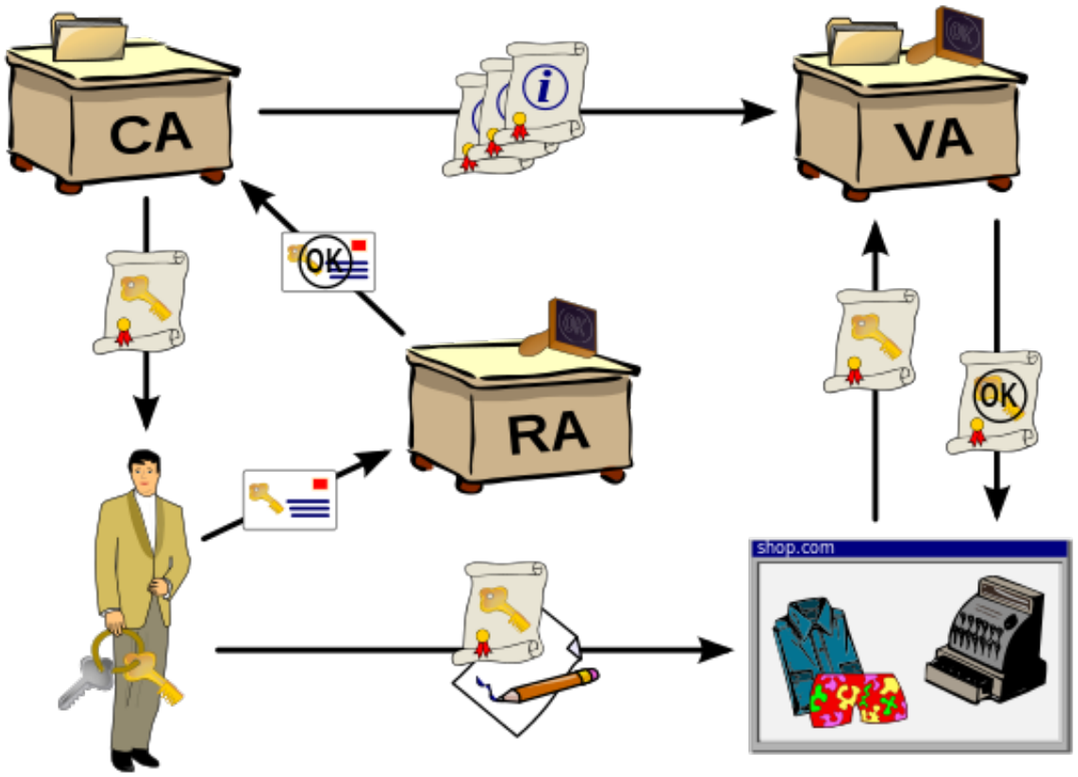
信任

RSA

VERISIGN™



公钥管理的P2P版本



PGP®

1991

GnuPG

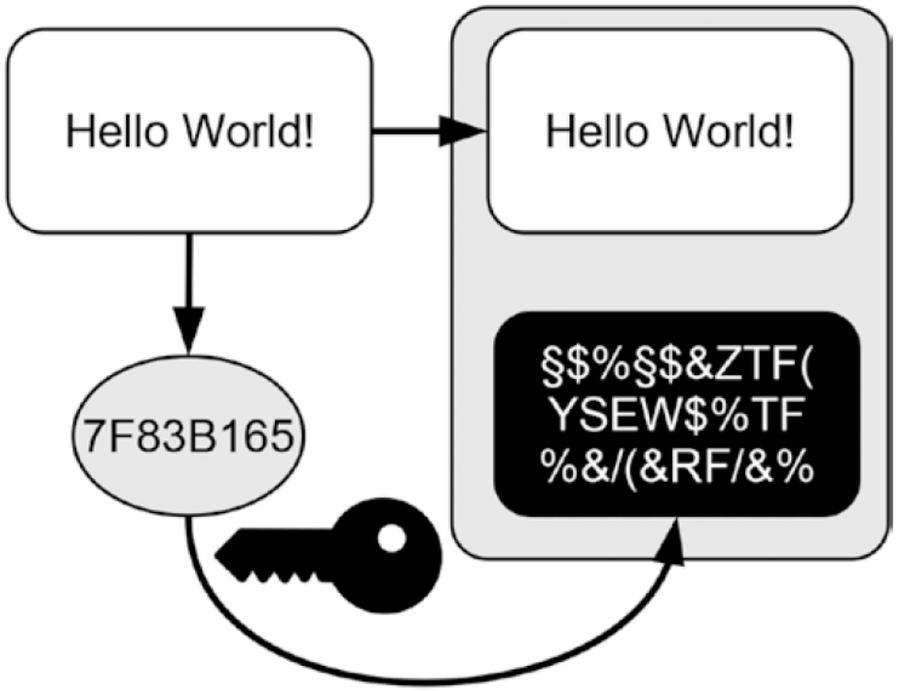
1999

Phil Zimmermann

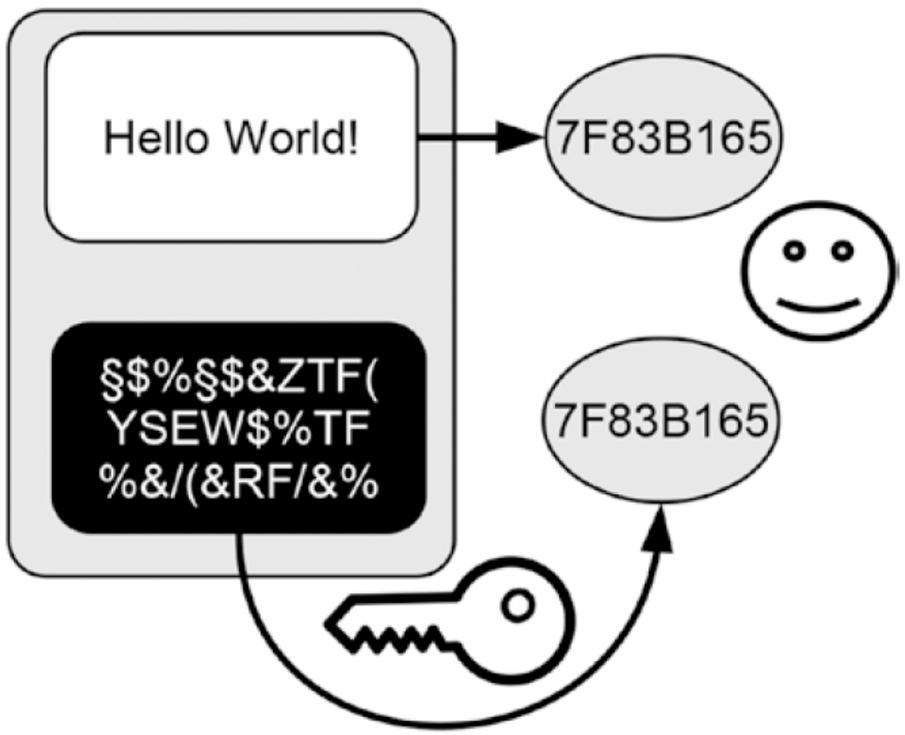
数字签名

Blockchain Basics:A Non-Technical Introduction in 25 Steps @ APRESS

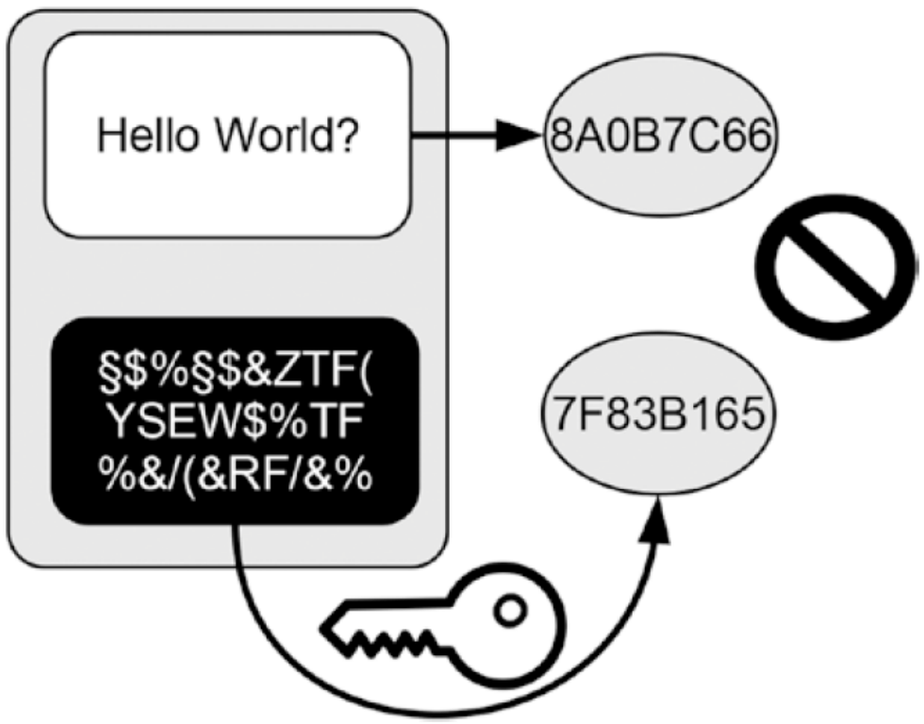
产生签名



验证签名



发现欺骗



自己签名，任何人都可以验证（公钥分发）

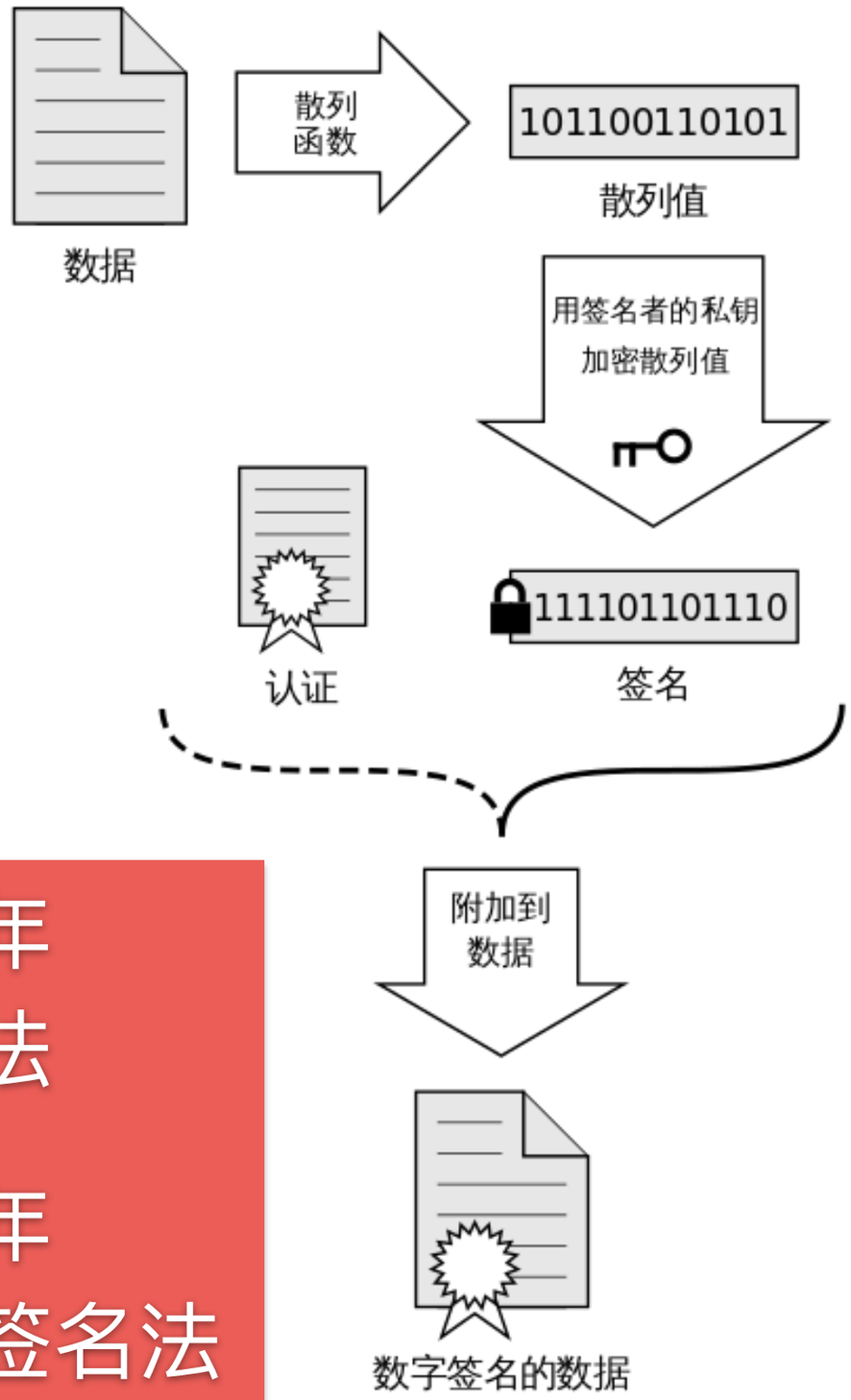
不可伪造，公钥私钥

签名信息的大小

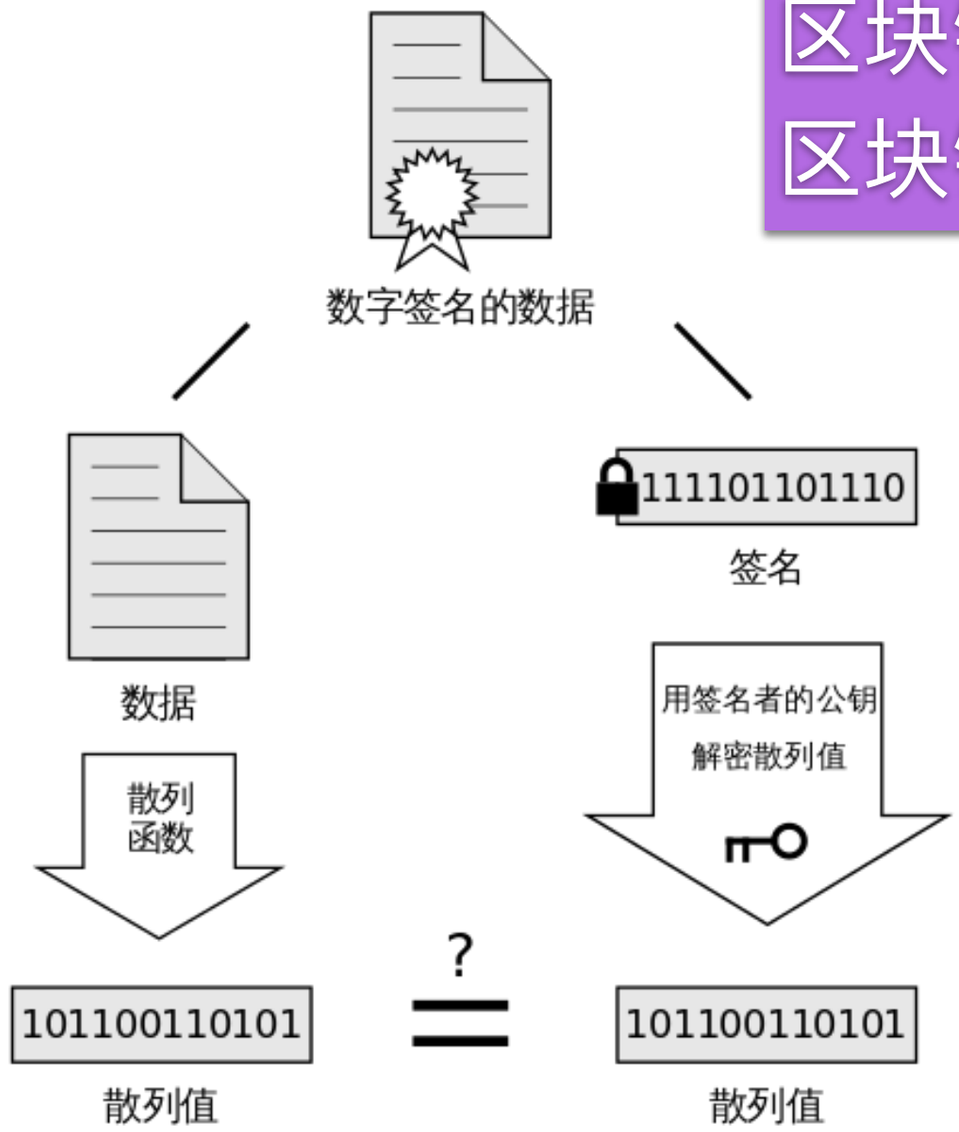
数字签名

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

签名



验证



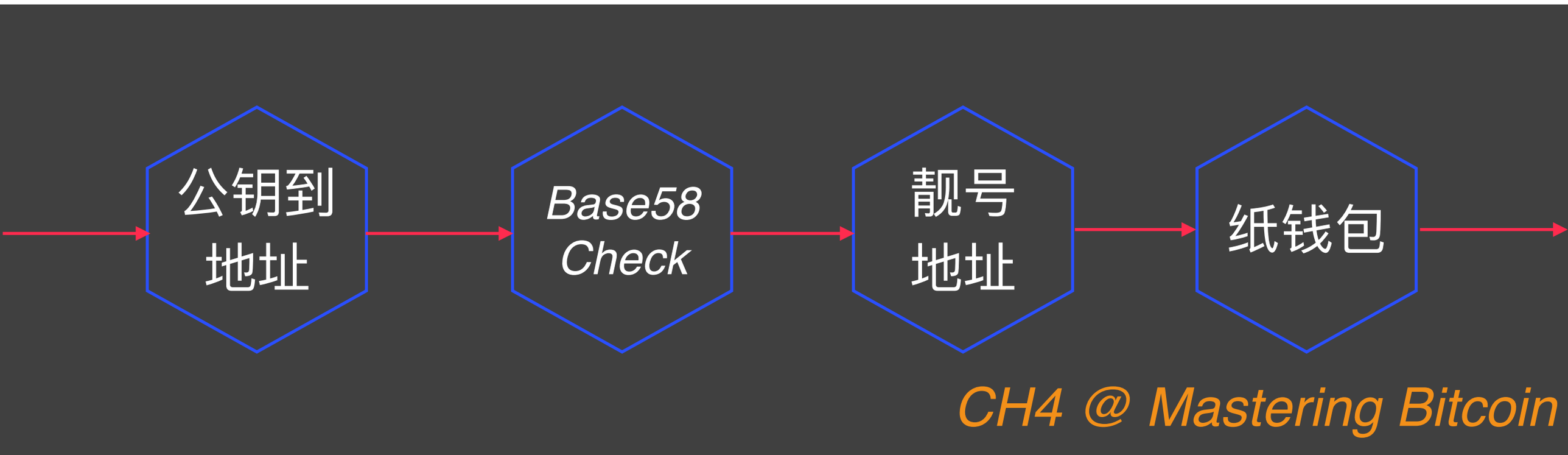
若两者的散列值一致，则此数字签名为有效

区块链存证
区块链公证

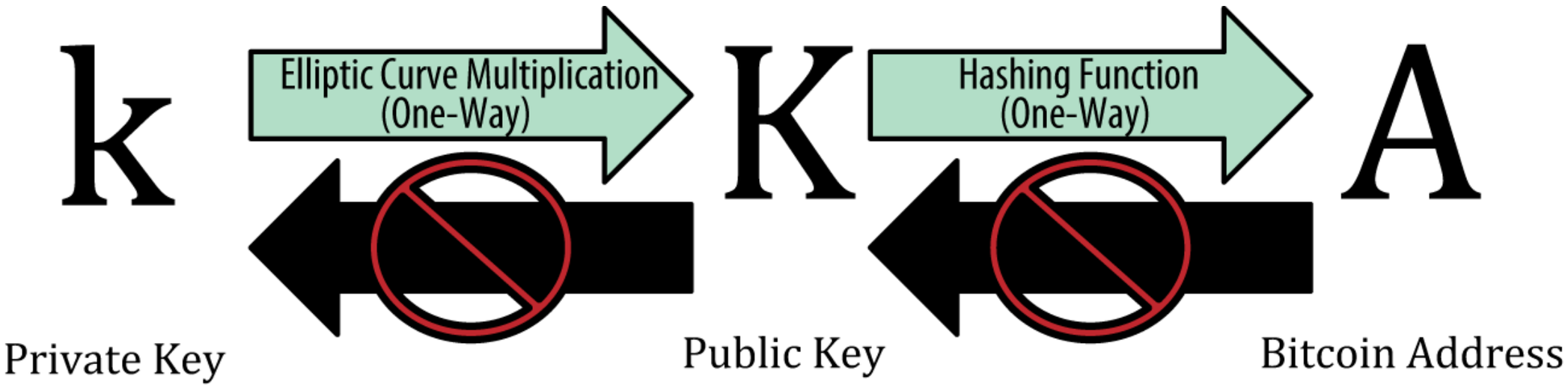
2000年
合同法

2005年
电子签名法

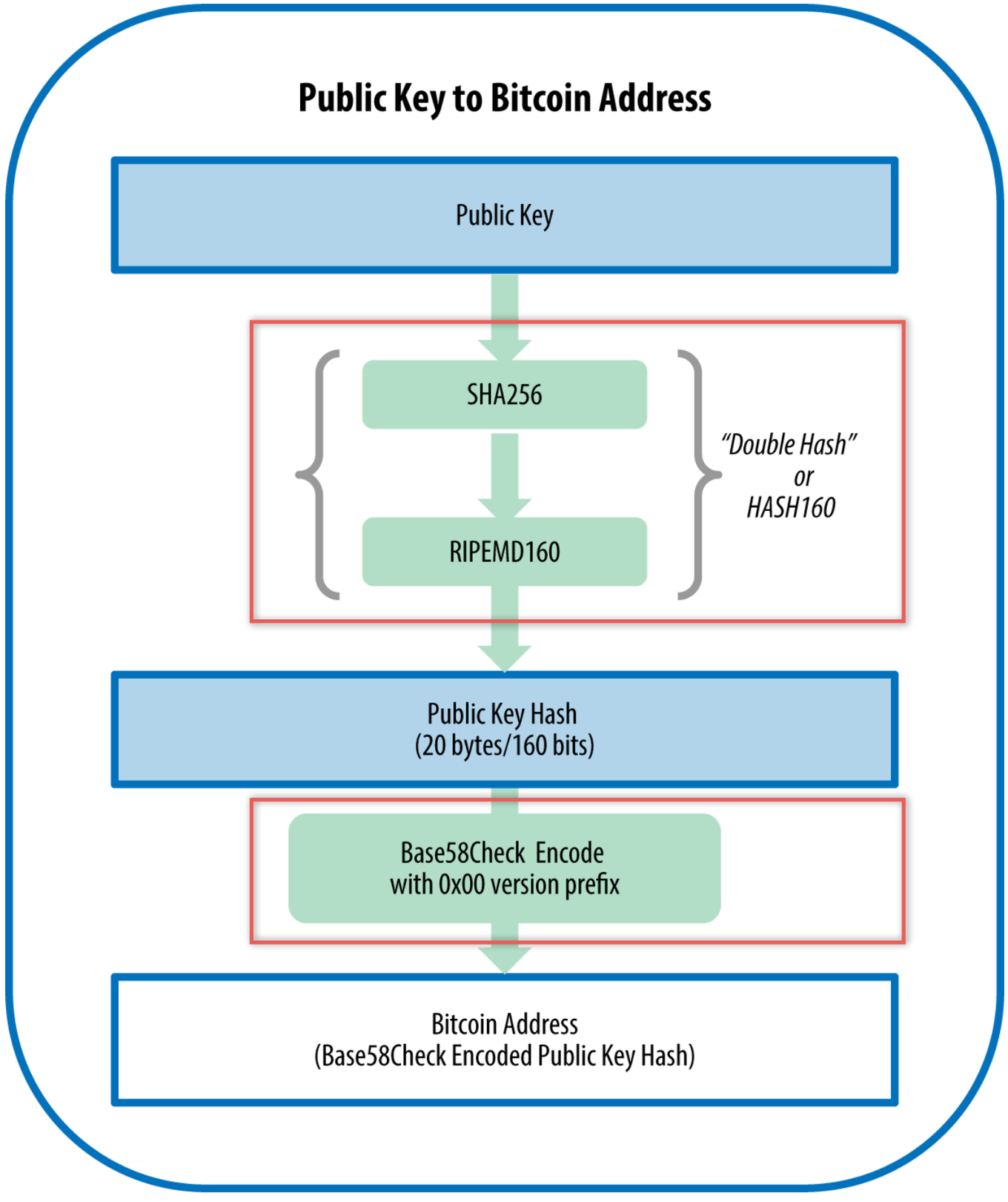
密钥和地址



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

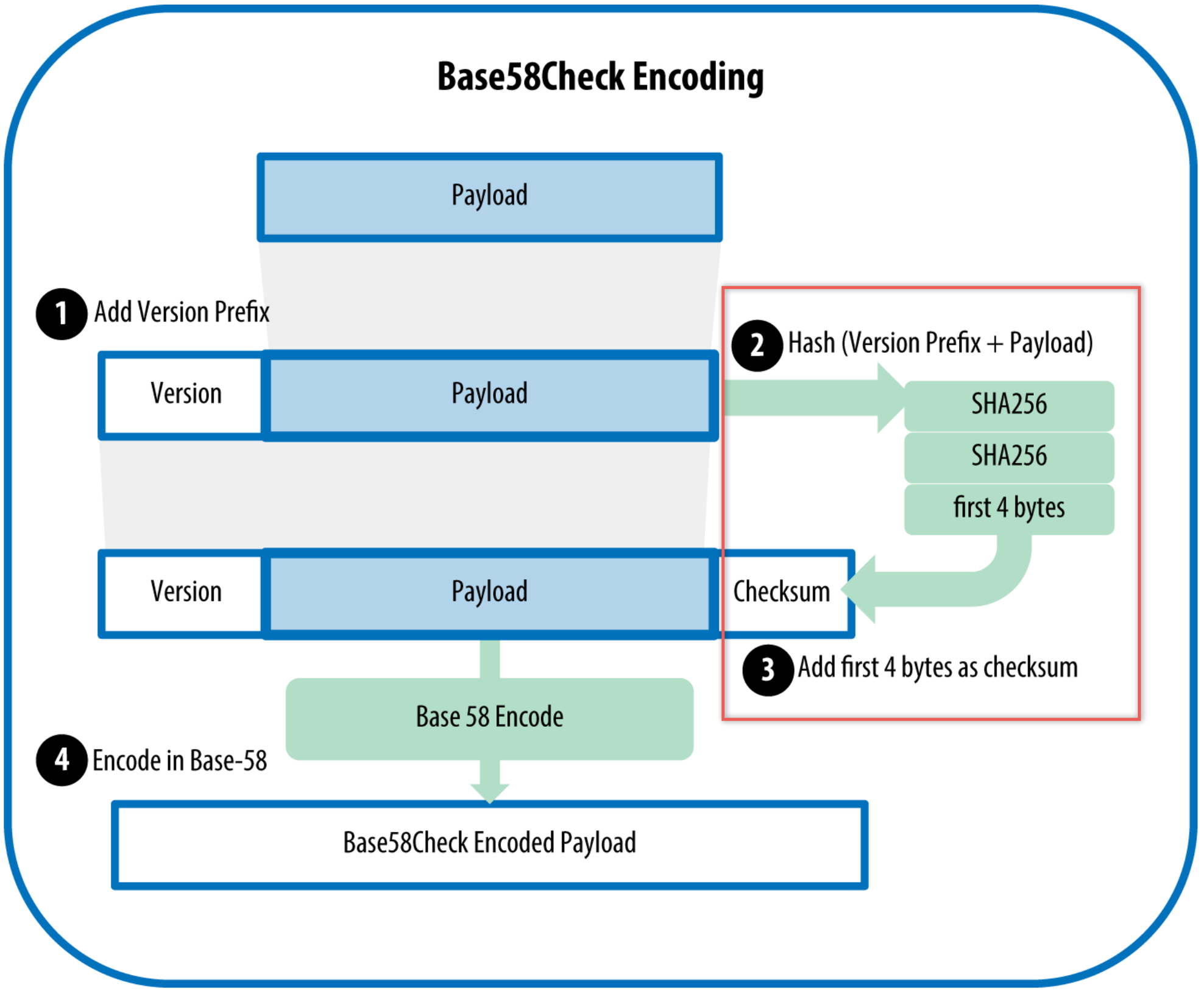
- 大写字母
- 小写字母
- 数字
- +、/

Base58

- 0和o
- I和l

Base58Check

- 检验和

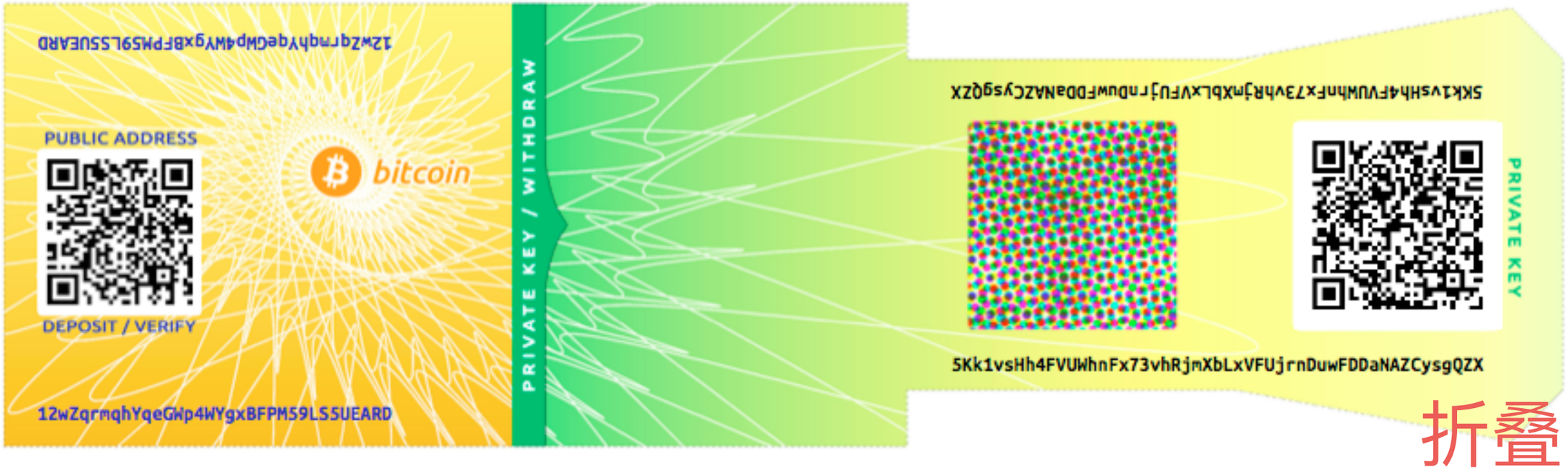


靓号地址

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



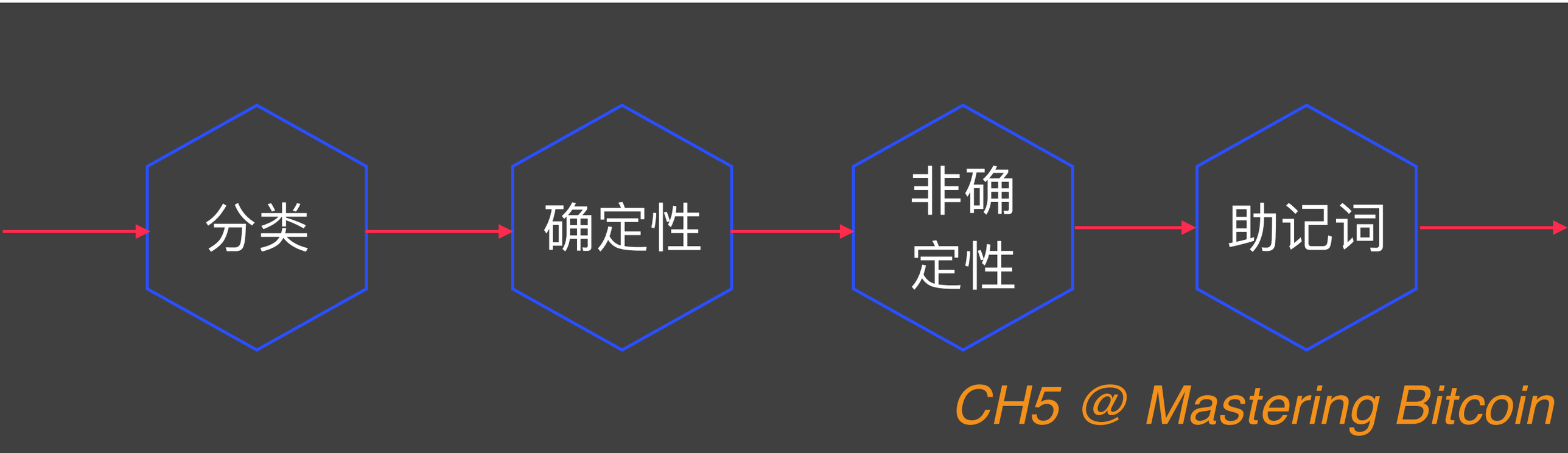
折叠

纸钱包

私钥
密封

多个副本

钱包



钱包

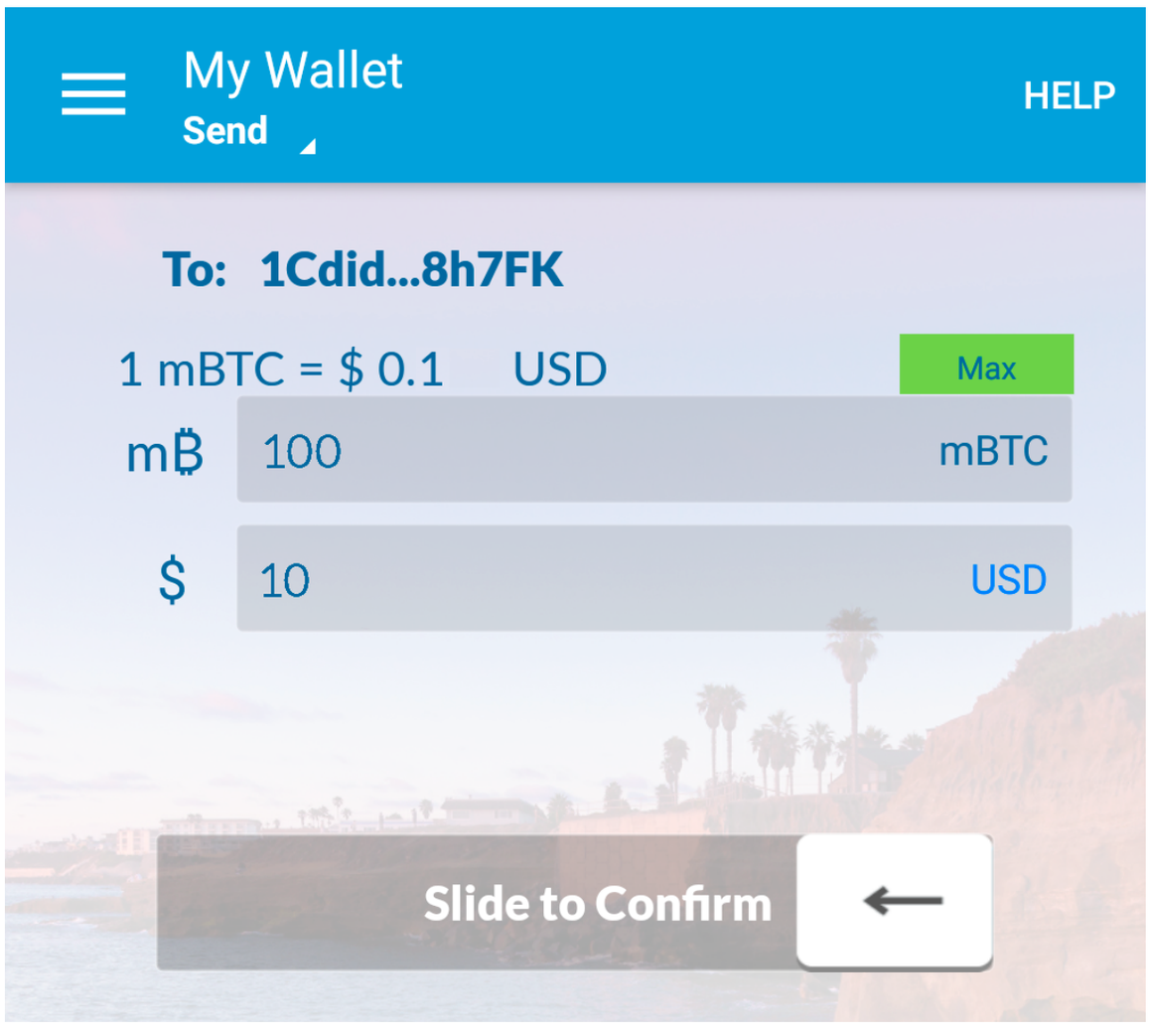
桌面钱包

手机钱包

网络钱包

硬件钱包

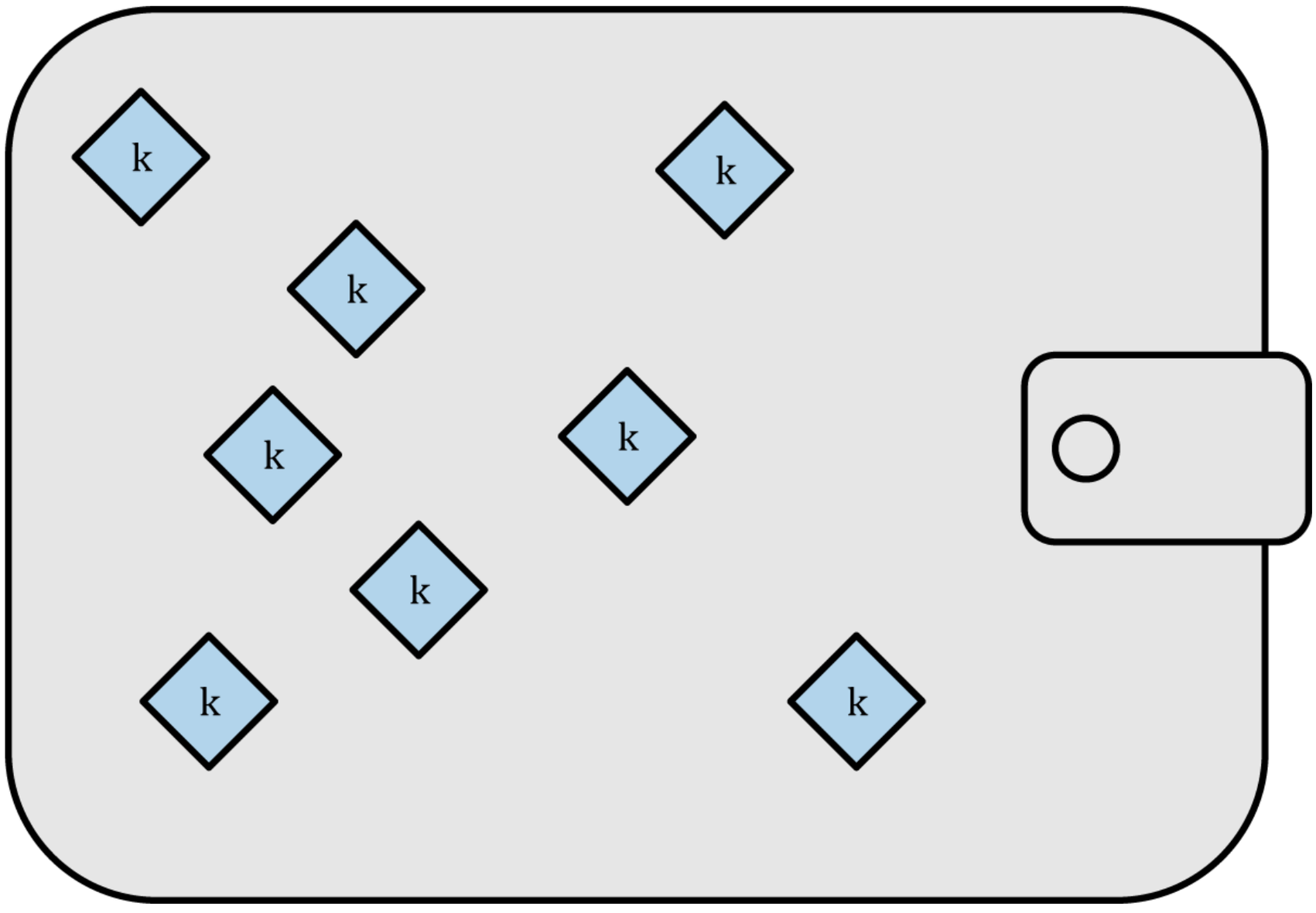
纸钱包



非确定性钱包

随机钱包

JBOK
Just a Bunch of Keys

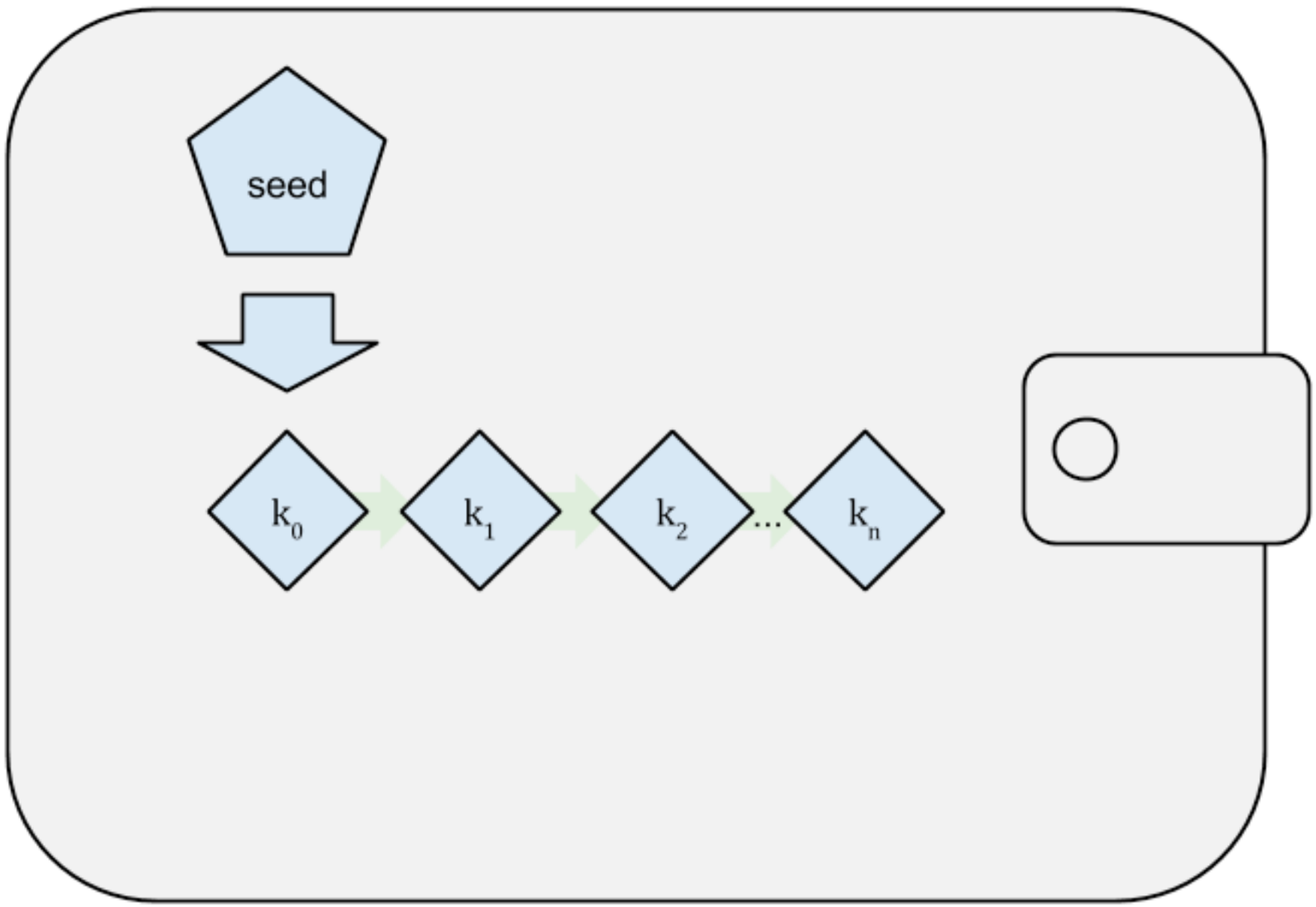


难于管理、备份和导入

确定性钱包

种子钱包

种子
—串随机生
成的数字

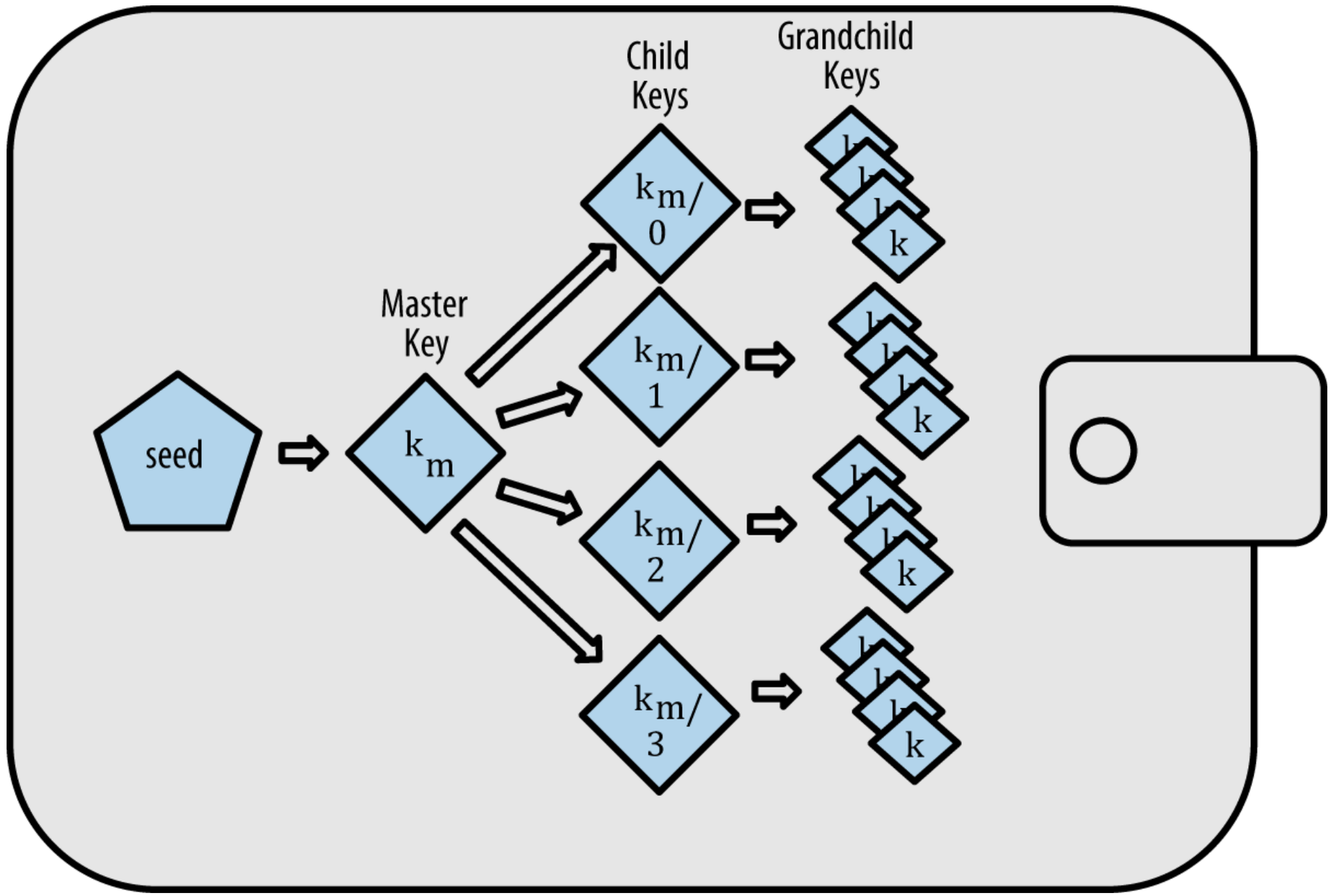


分层确定性钱包

HD钱包

BIP-32
BIP-43
BIP-44

BIP-39

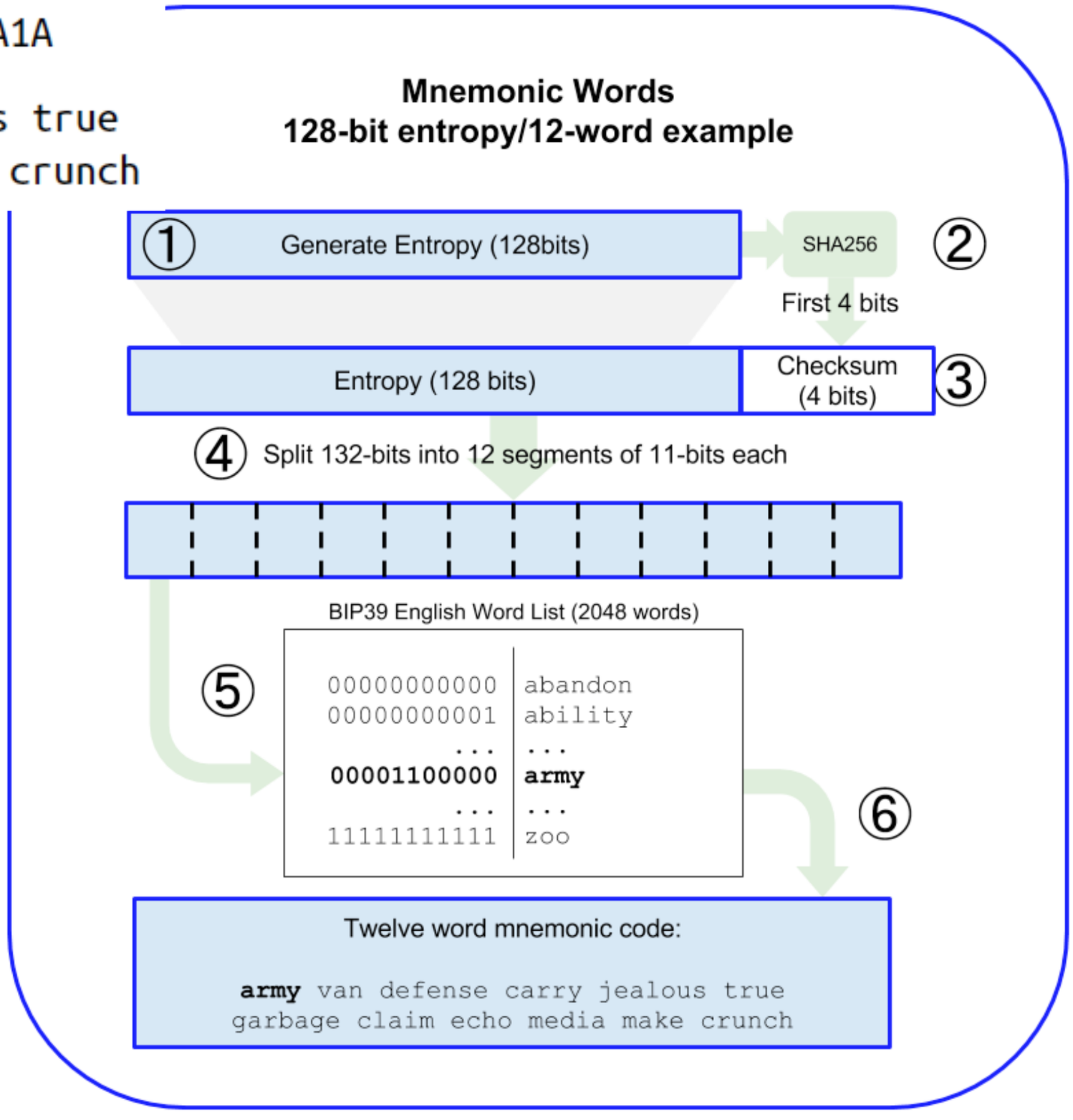


助记词

```
0C1E24E5917779D297E14D45F14E1A1A

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

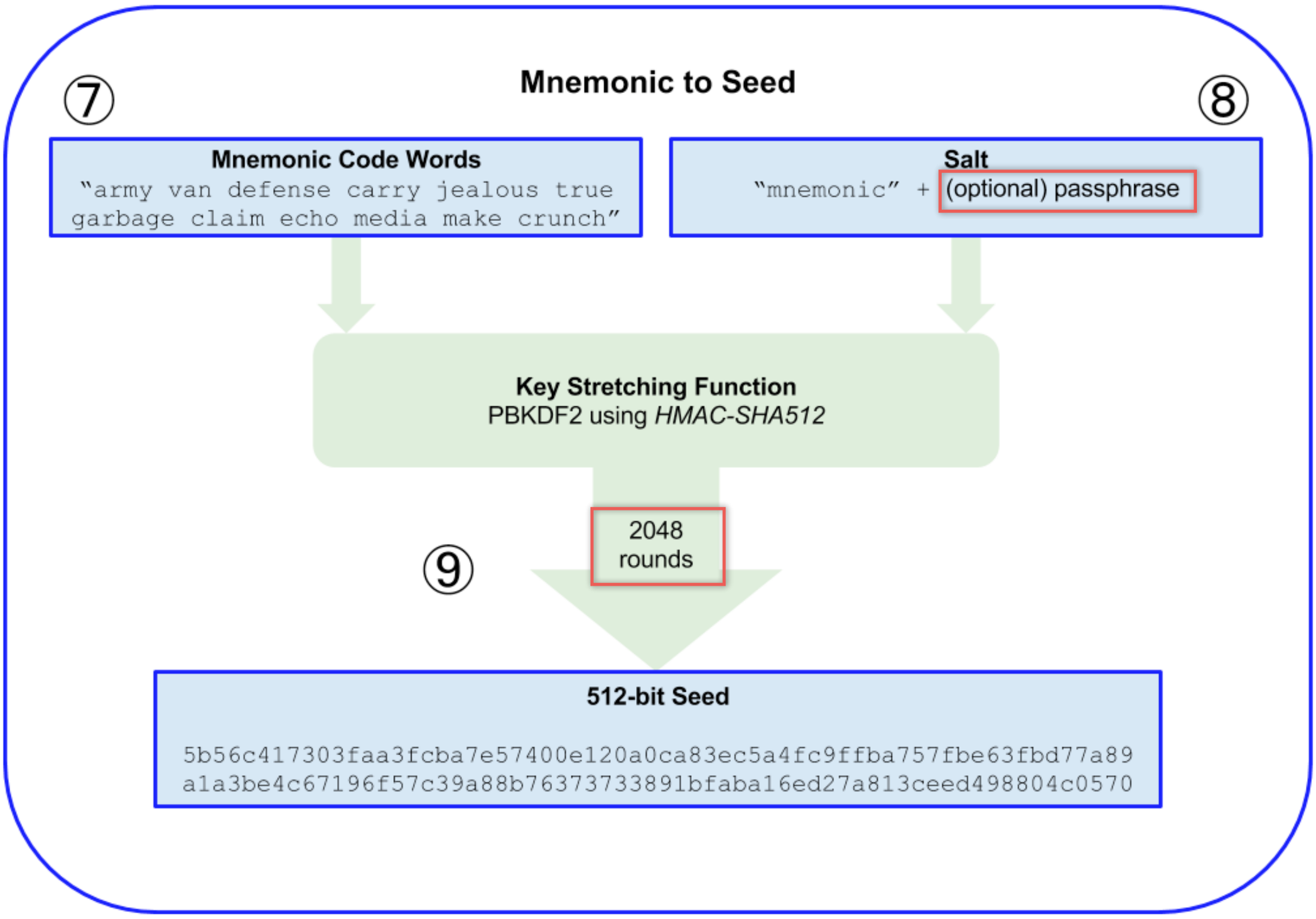
1. *army*
2. *van*
3. *defense*
4. *carry*
5. *jealous*
6. *true*
7. *garbage*
8. *claim*
9. *echo*
10. *media*
11. *make*
12. *crunch*



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

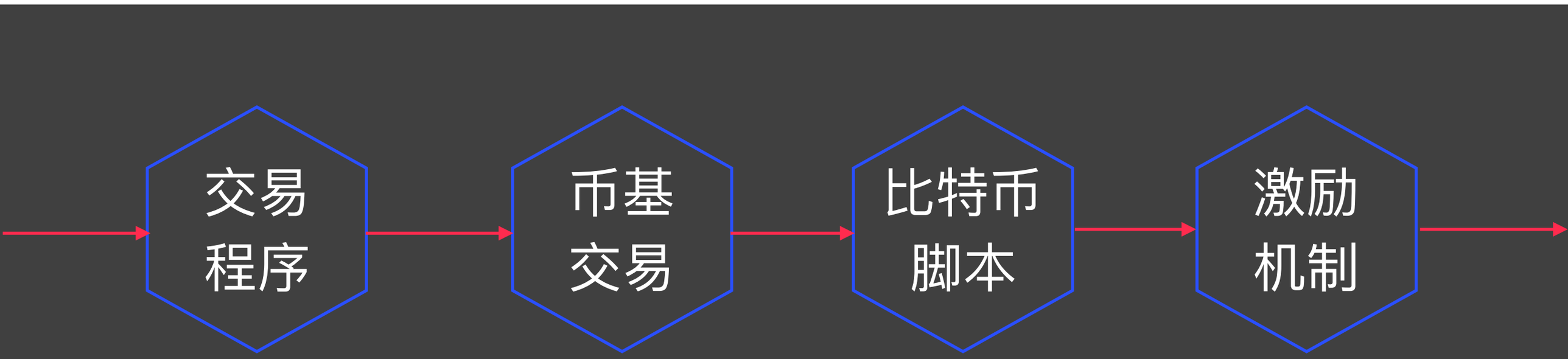
Bitcoin

BIP32 Root Key

xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6
i6ddYjb5PLtUdMZn8LhvuCVhGcQntq5rn7JVMqnie

https://iancoleman.io/bip39/

比特币交易



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"
   }
  ]
}
```

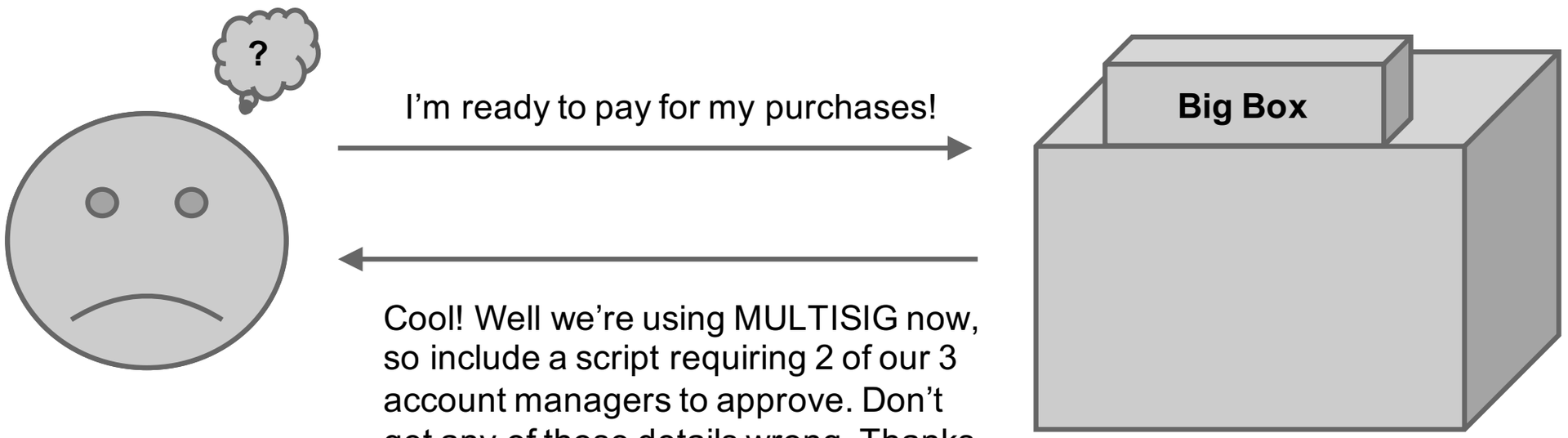
图3.3 一个真实的比特币交易程序段

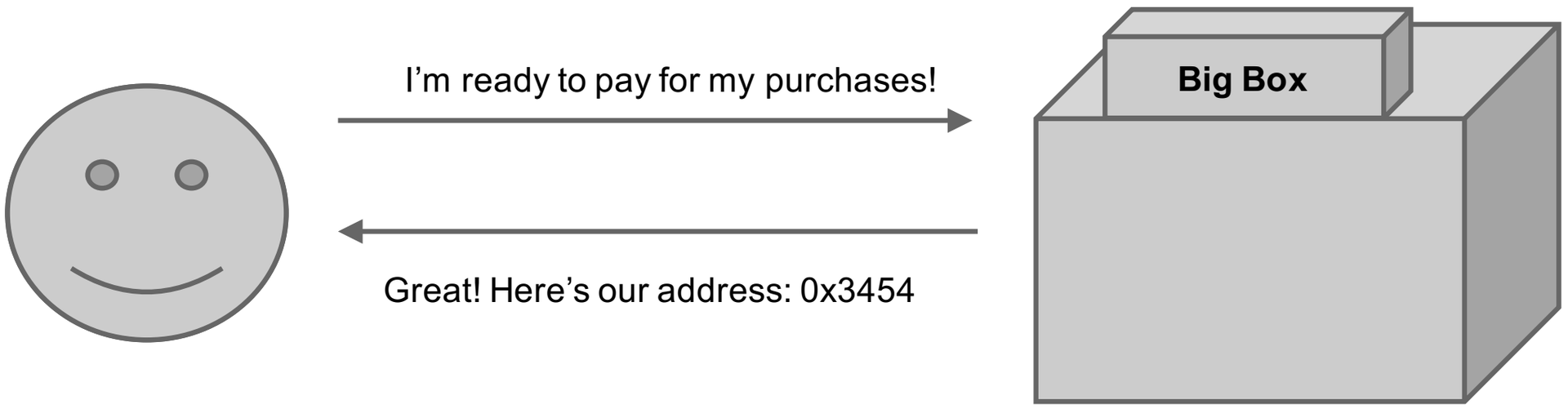
币基交易

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

图3.8 币基交易

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
```

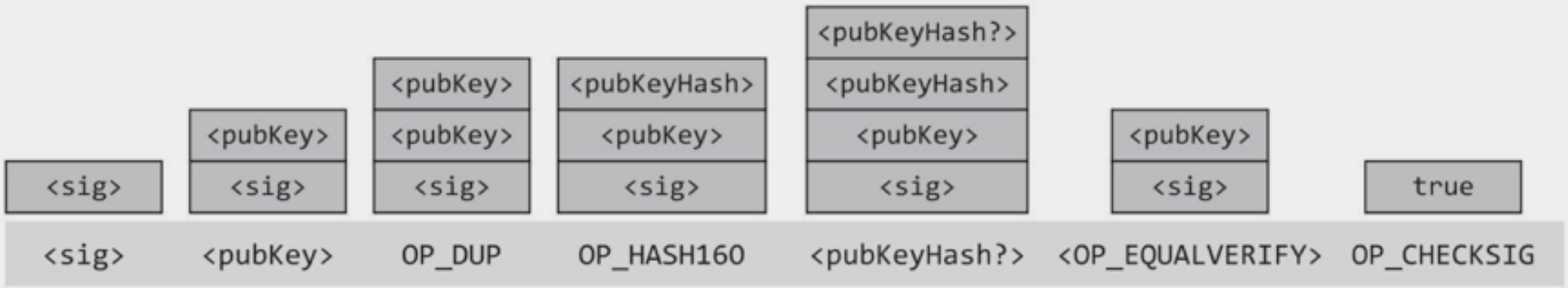
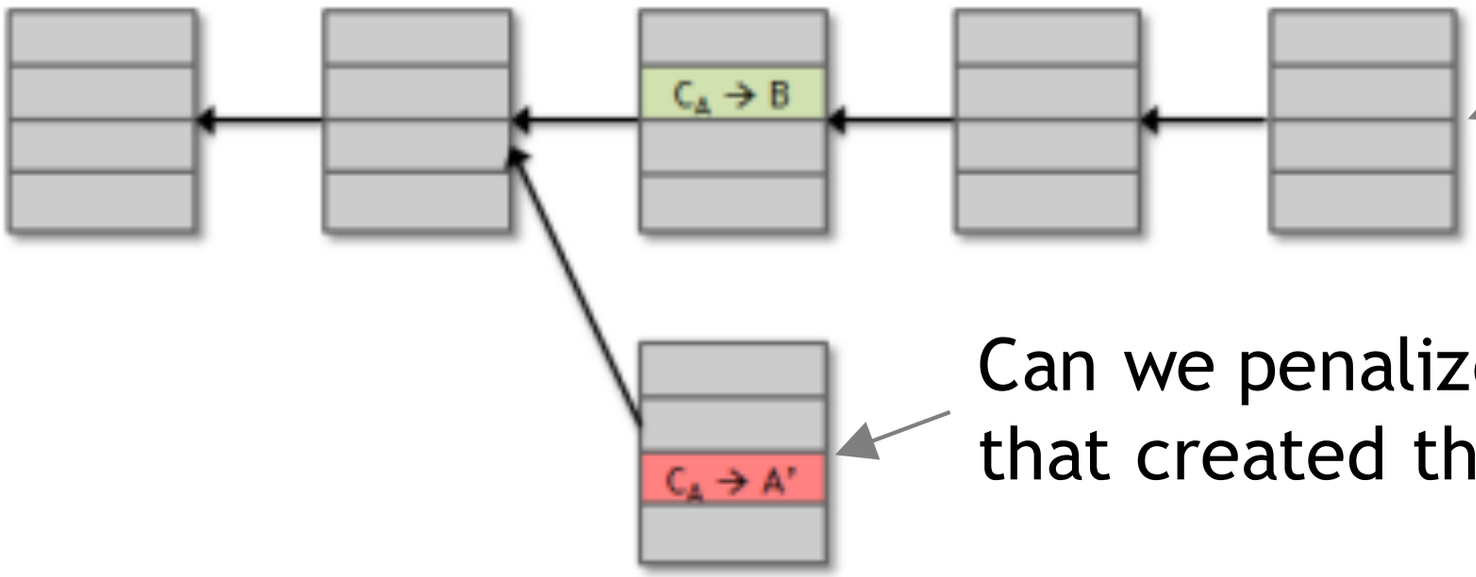


图3.6 比特币脚本的执行堆栈状态图

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。

激励节点诚实



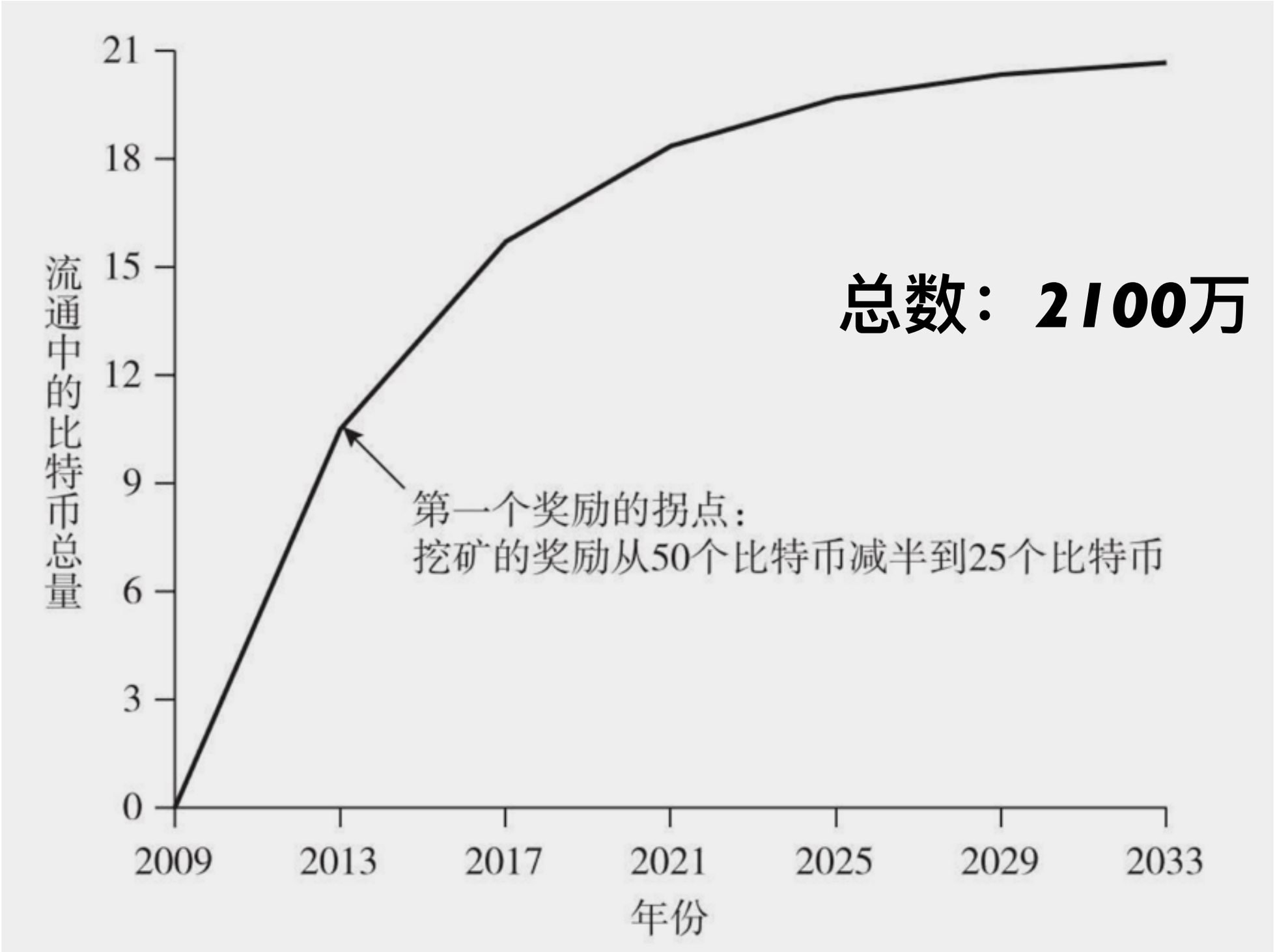
Can we reward nodes that created these blocks?

Can we penalize the node that created this block?

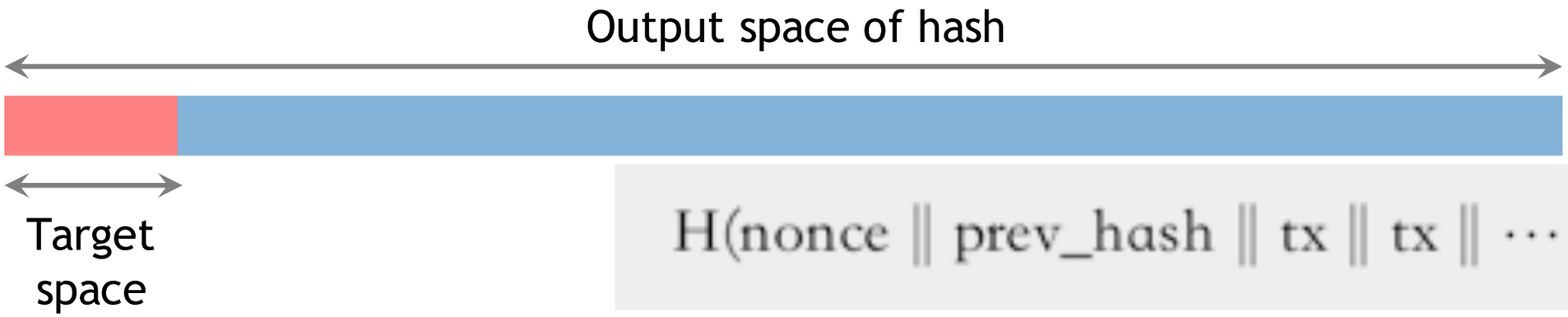
区块奖励 *vs.* 交易费奖励

交易费：输入和输出不等

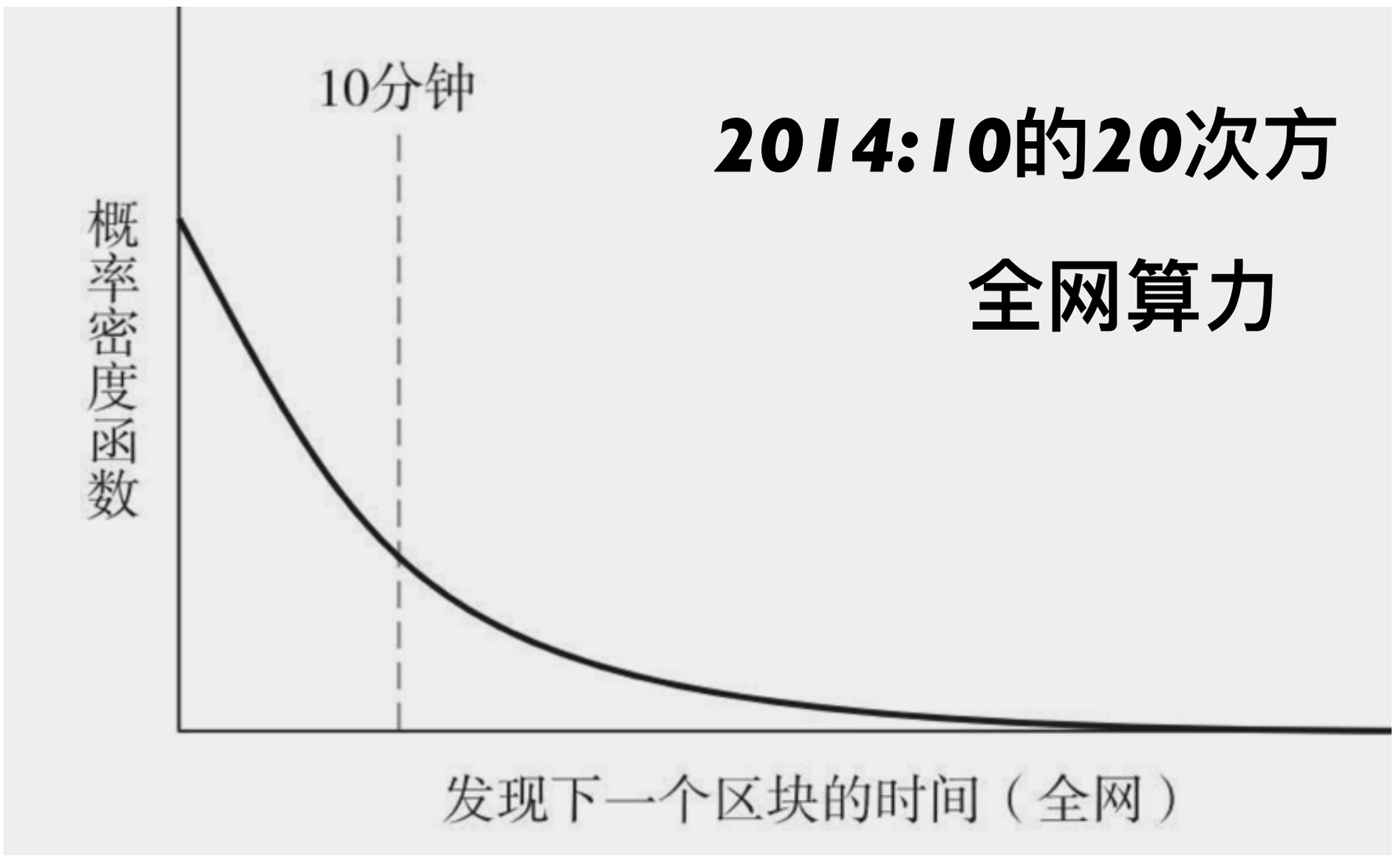
比特币奖励


21
18
15
12
9
6
3
0
流通中的比特币总量
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

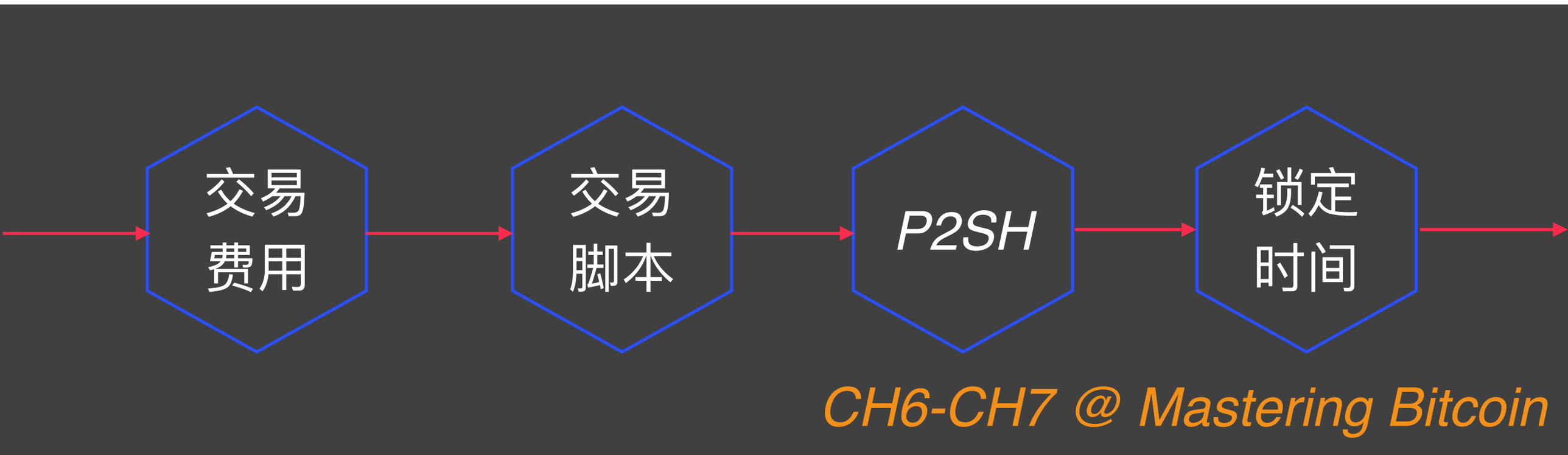
限定*Hash*的输出范围

临时随机数

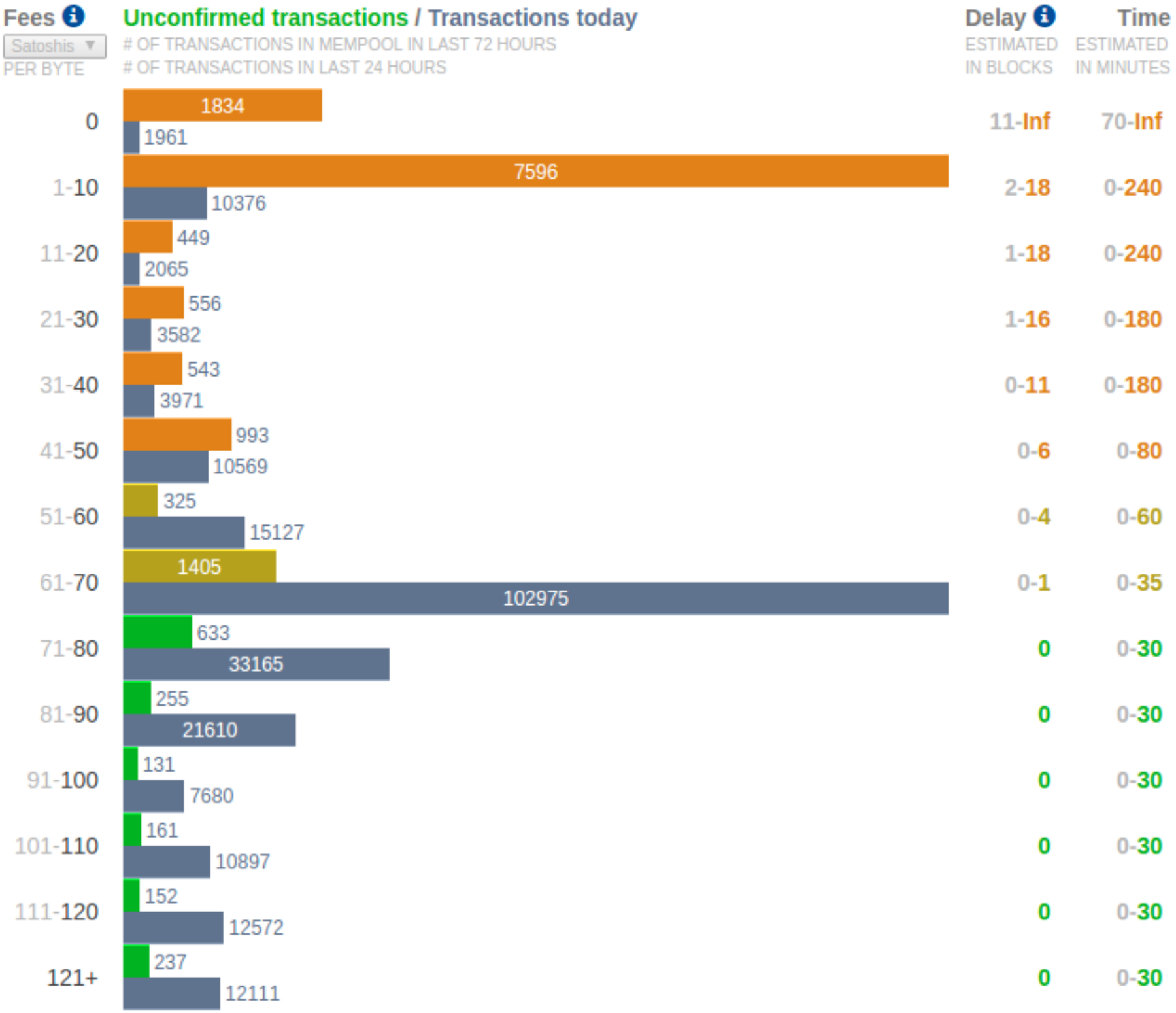
***PoW*：**
工作量证明

***PoS*：**
权益证明

交易



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

交易脚本

Unlocking Script (scriptSig) + Locking Script (scriptPubKey)

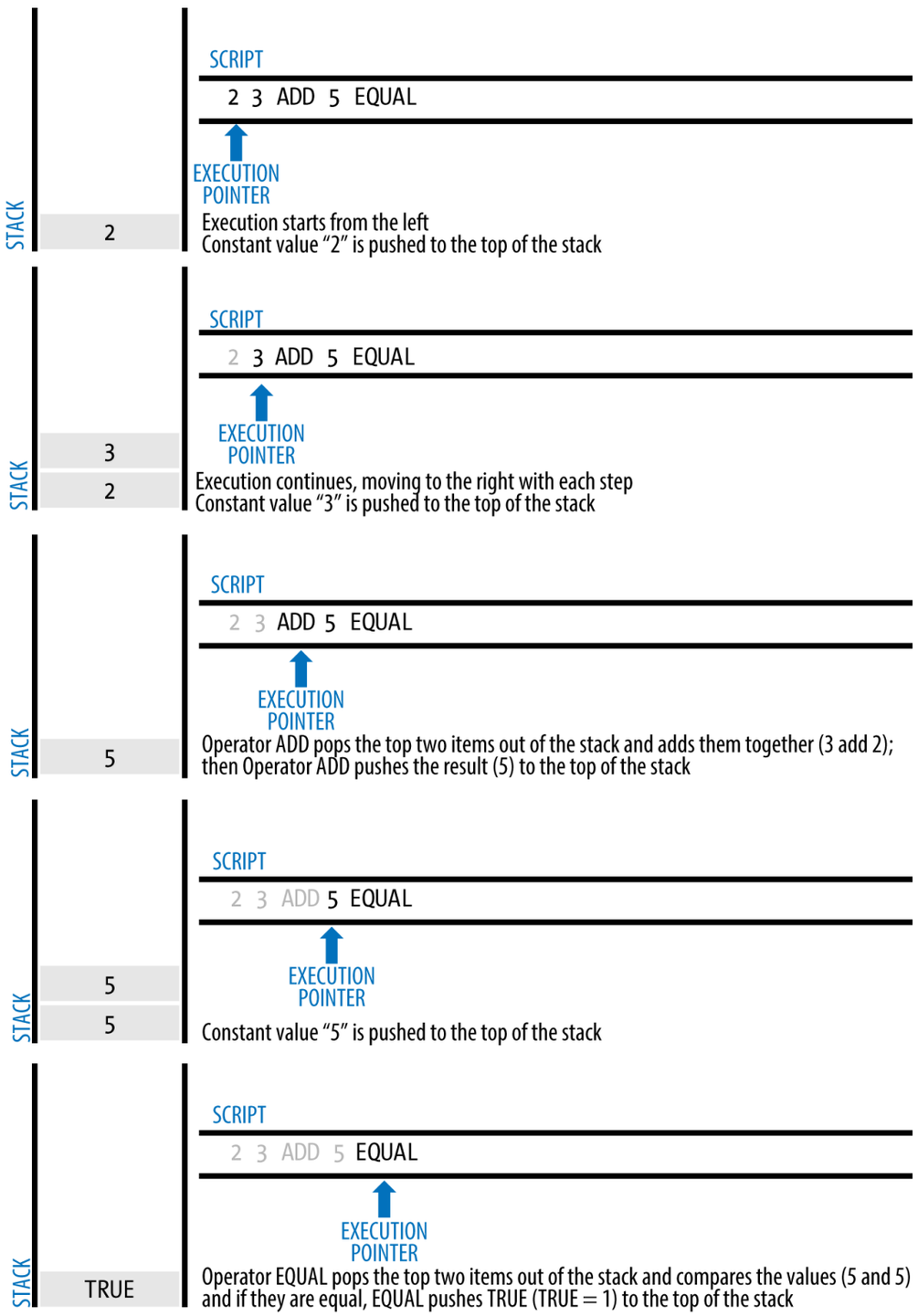
```
<sig> <PubK>
```

Unlock Script (scriptSig) is provided by the user to resolve the encumbrance

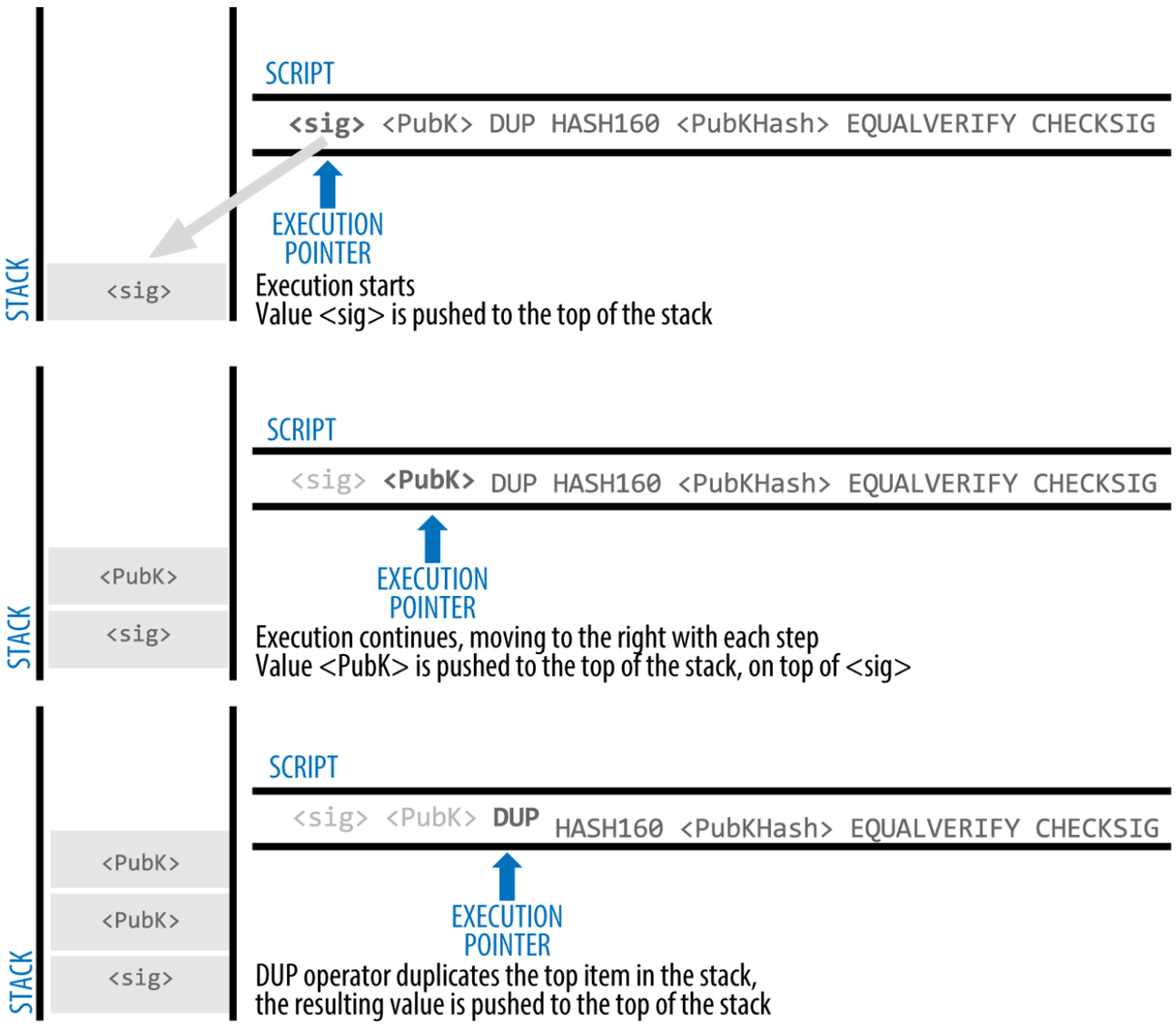
```
DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
```

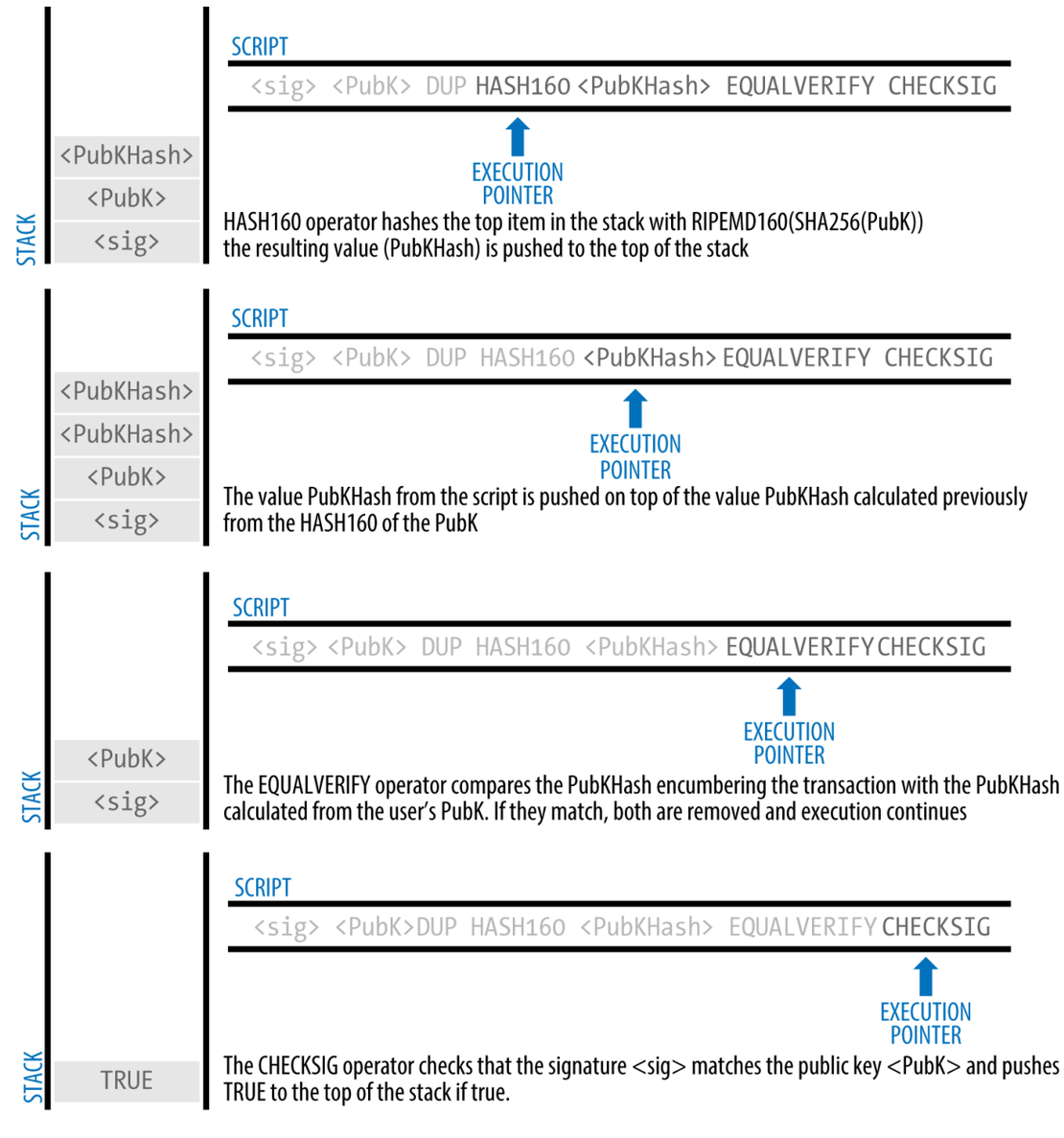
Lock Script (scriptPubKey) is found in a transaction output and is the encumbrance that must be fulfilled to spend the output

交易脚本

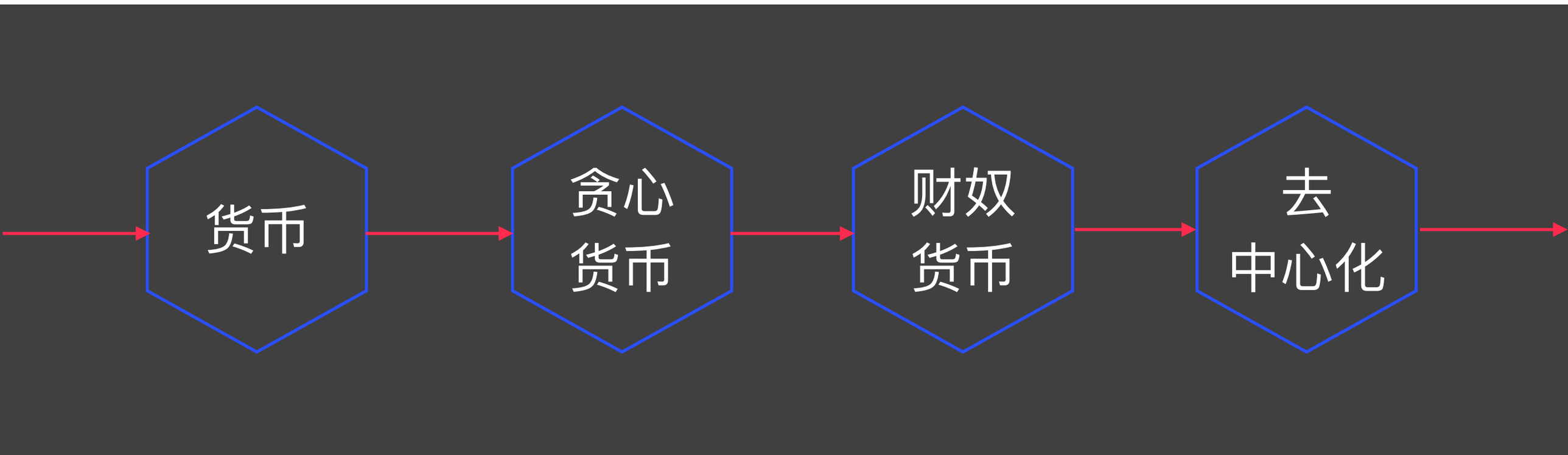

SCRIPT
2 3 ADD 5 EQUAL
EXECUTION POINTER
STACK
2
Execution starts from the left
Constant value "2" is pushed to the top of the stack
SCRIPT
2 3 ADD 5 EQUAL
EXECUTION POINTER
STACK
3
2
Execution continues, moving to the right with each step
Constant value "3" is pushed to the top of the stack
SCRIPT
2 3 ADD 5 EQUAL
EXECUTION POINTER
STACK
5
Operator ADD pops the top two items out of the stack and adds them together (3 add 2); then Operator ADD pushes the result (5) to the top of the stack
SCRIPT
2 3 ADD 5 EQUAL
EXECUTION POINTER
STACK
5
5
Constant value "5" is pushed to the top of the stack
SCRIPT
2 3 ADD 5 EQUAL
EXECUTION POINTER
STACK
TRUE
Operator EQUAL pops the top two items out of the stack and compares the values (5 and 5) and if they are equal, EQUAL pushes TRUE (TRUE = 1) to the top of the stack

交易脚本


SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<sig>
Execution starts
Value <sig> is pushed to the top of the stack
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<sig>
Execution continues, moving to the right with each step
Value <PubK> is pushed to the top of the stack, on top of <sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<PubK>
<sig>
DUP operator duplicates the top item in the stack,
the resulting value is pushed to the top of the stack


SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubKHash>
<PubK>
<sig>
HASH160 operator hashes the top item in the stack with RIPEMD160(SHA256(PubK))
the resulting value (PubKHash) is pushed to the top of the stack
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubKHash>
<PubKHash>
<PubK>
<sig>
The value PubKHash from the script is pushed on top of the value PubKHash calculated previously
from the HASH160 of the PubK
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
<PubK>
<sig>
The EQUALVERIFY operator compares the PubKHash encumbering the transaction with the PubKHash
calculated from the user's PubK. If they match, both are removed and execution continues
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
STACK
TRUE
The CHECKSIG operator checks that the signature <sig> matches the public key <PubK> and pushes
TRUE to the top of the stack if true.

加密货币



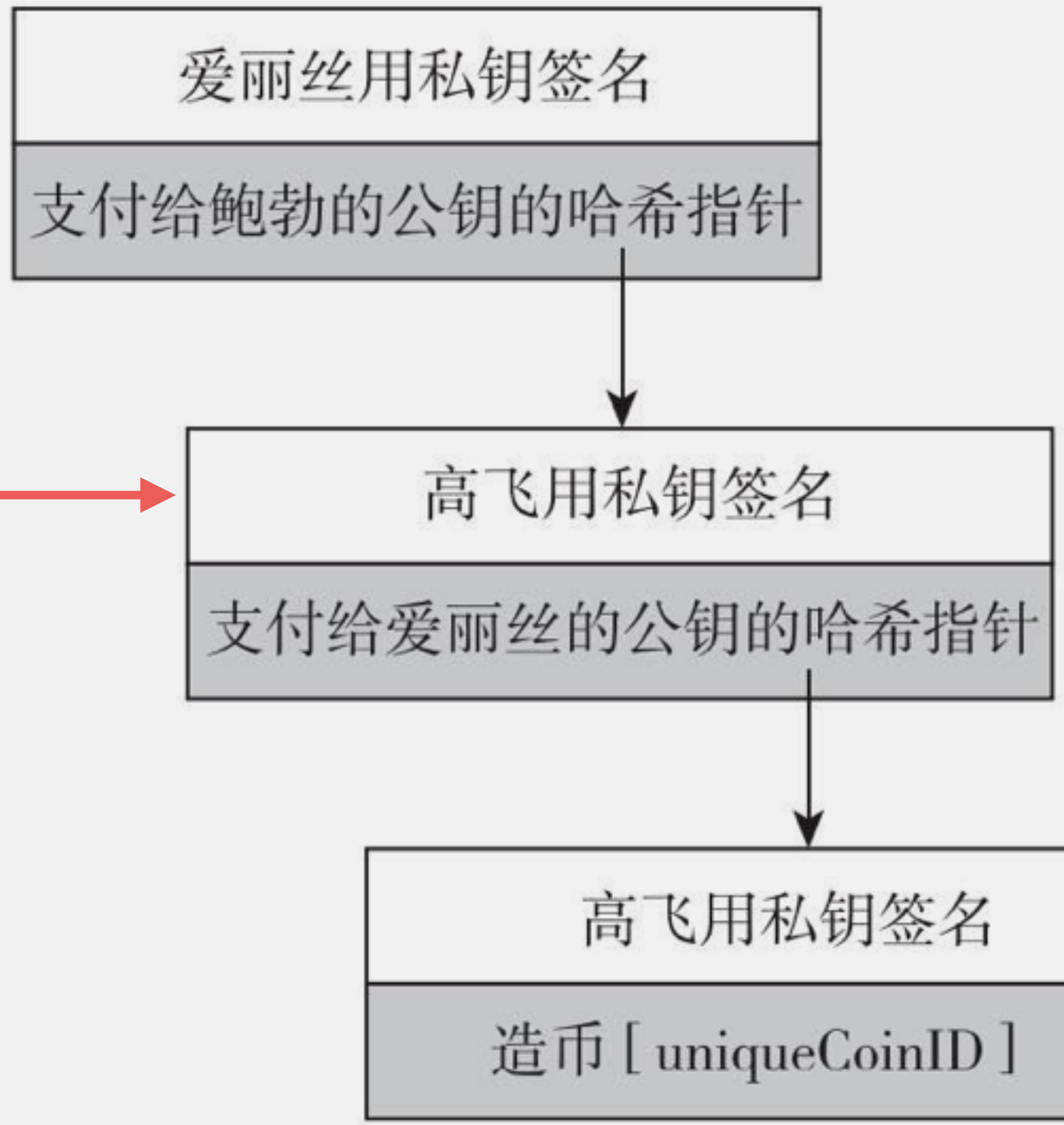
货币


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
样币禁止流通
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。
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，课件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面额数字“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。
广发银行
CGB

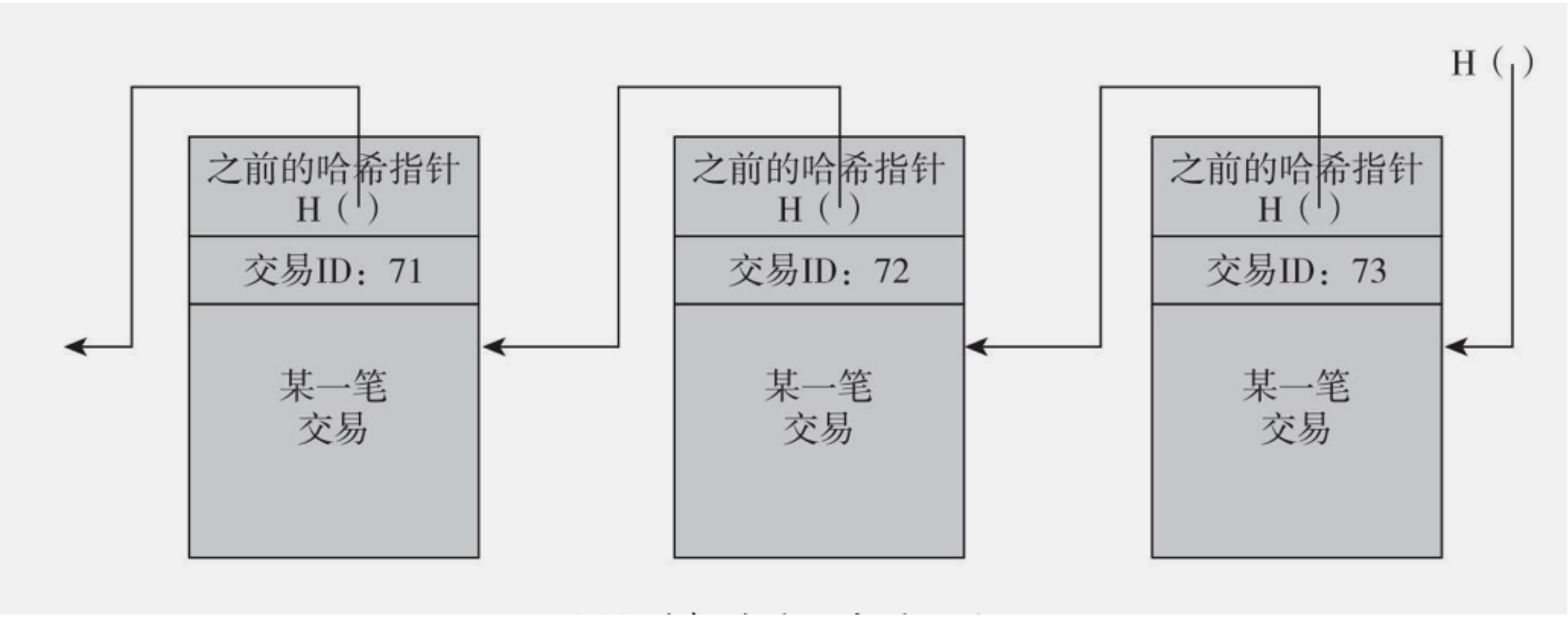
高飞币

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?

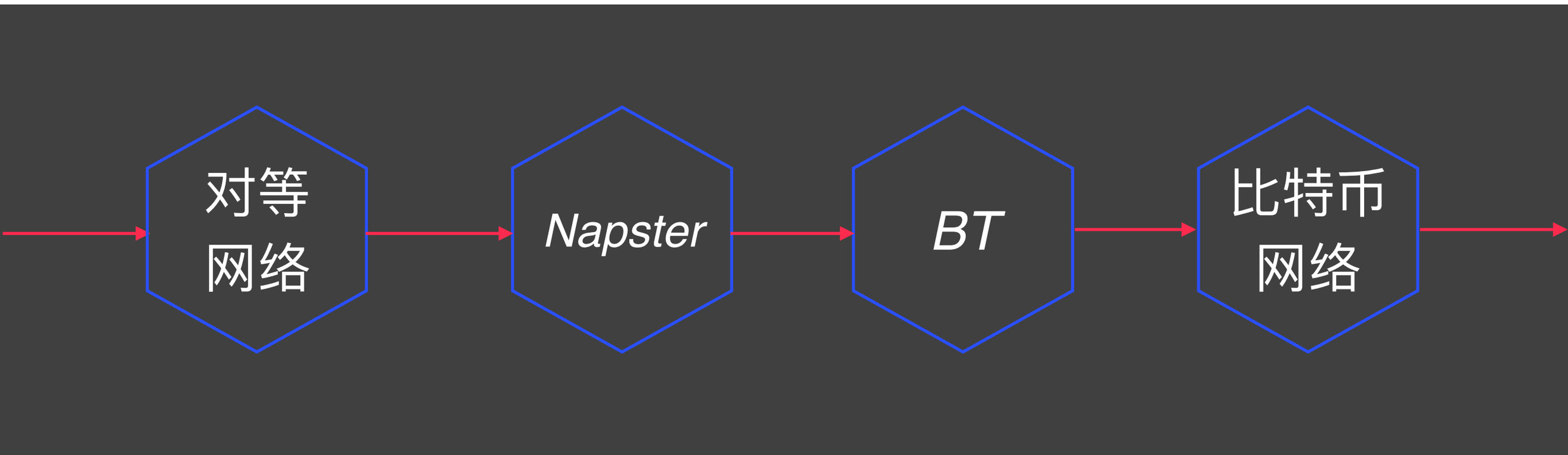
技术

- 谁决定系统如何改变规则?
- 比特币如何获得交易价格

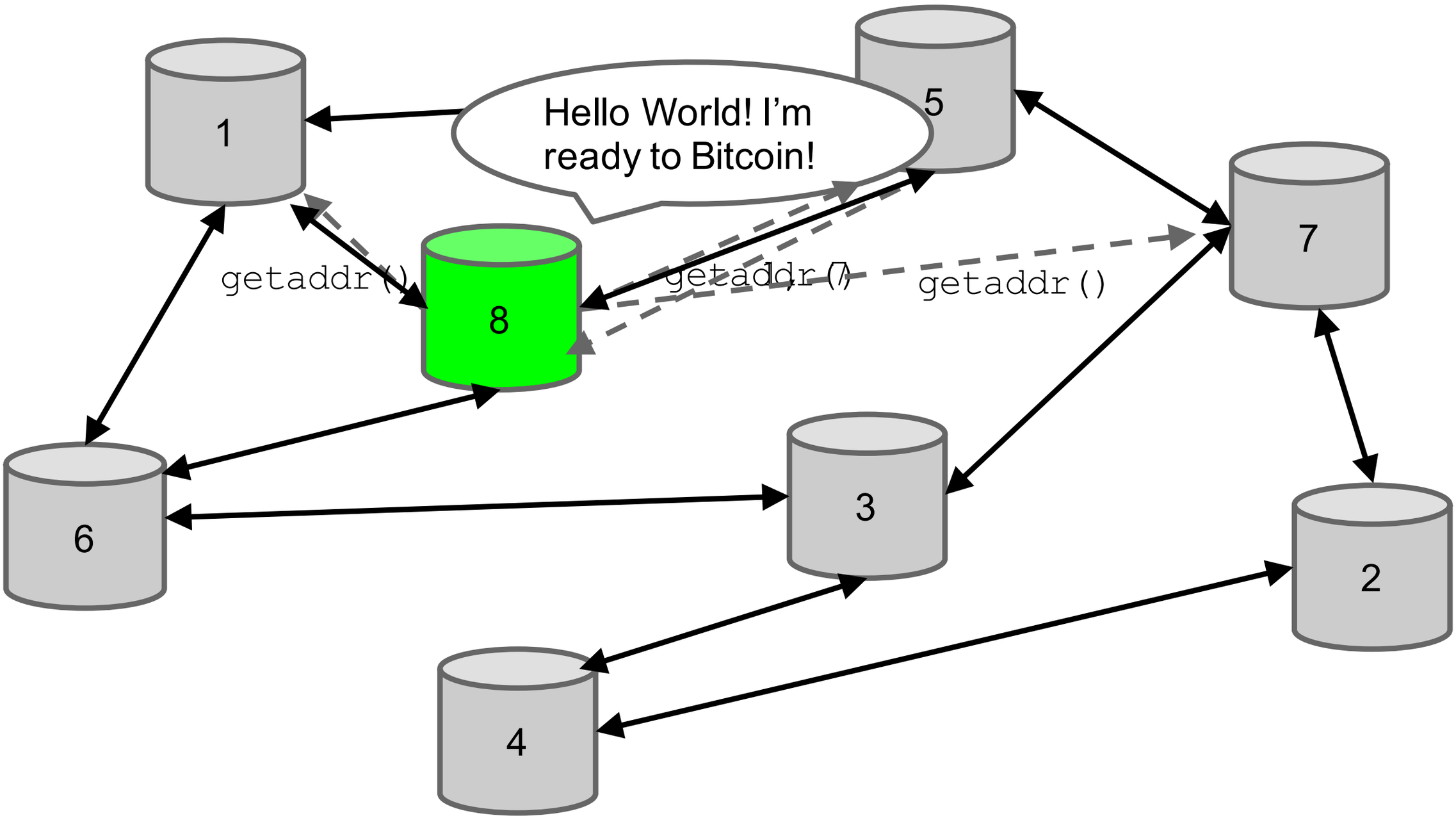
激励

用户:对等网络 矿工 挖矿 开发人员:软件更新

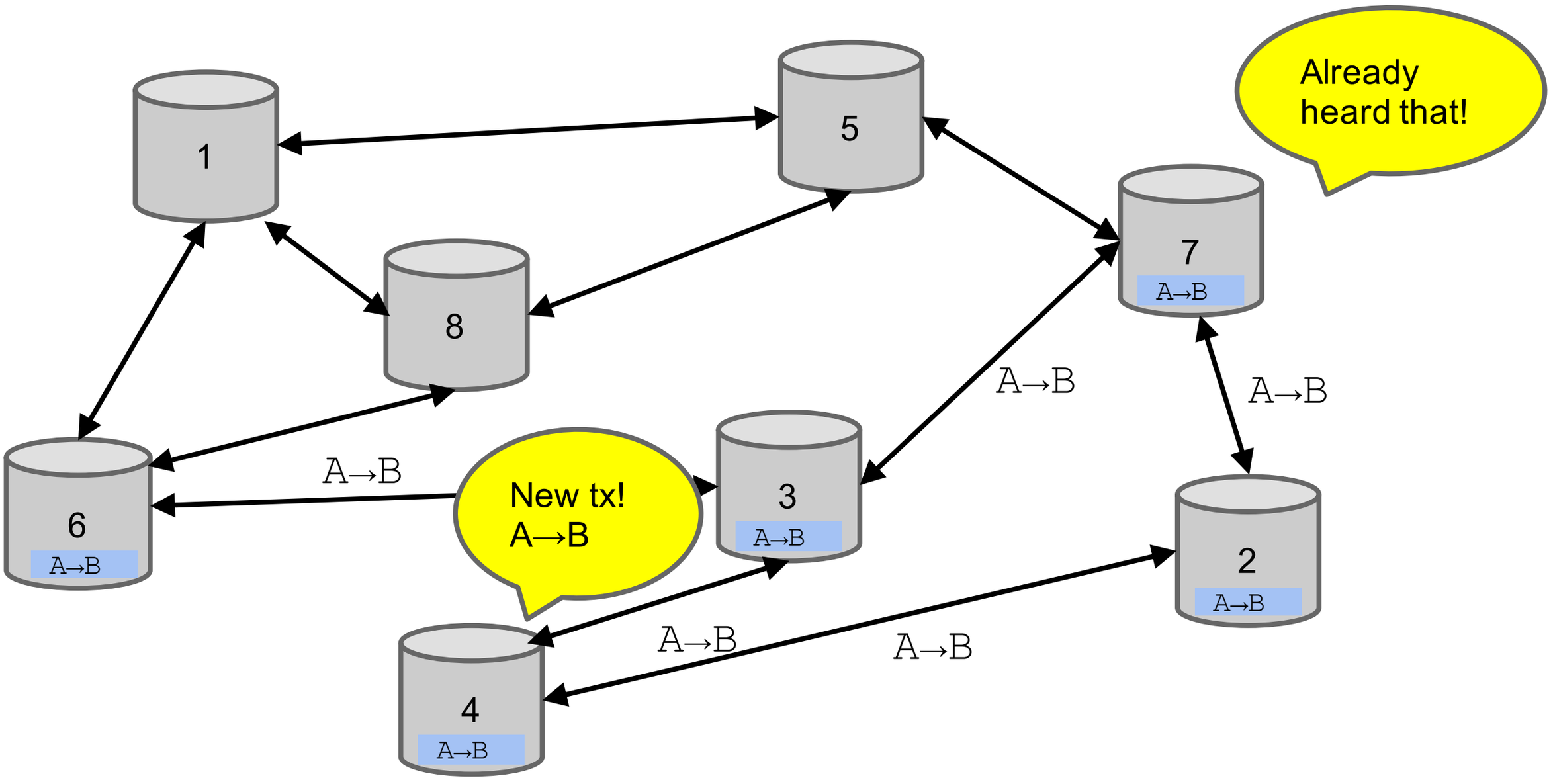
网络



比特币网络

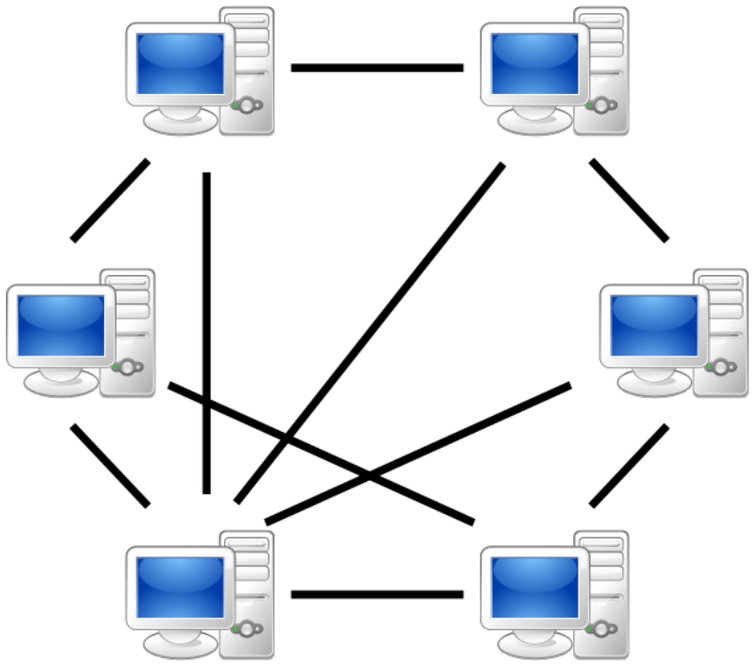

1
Hello World! I'm
ready to Bitcoin!
5
getaddr()
8
getaddr()
getaddr()
7
6
3
2
4

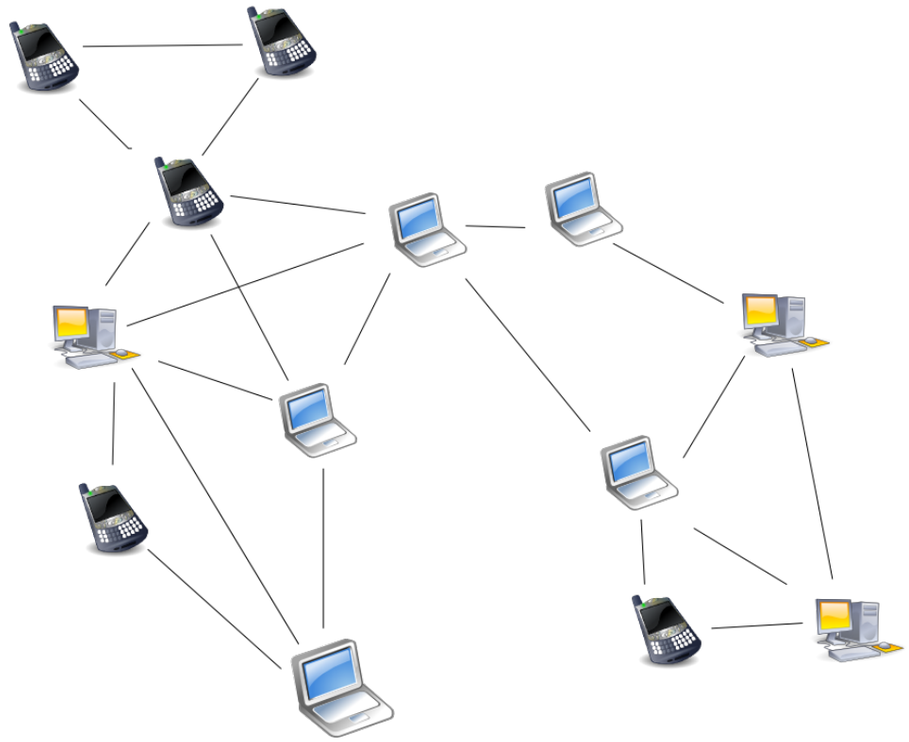
比特币网络交易消息传播

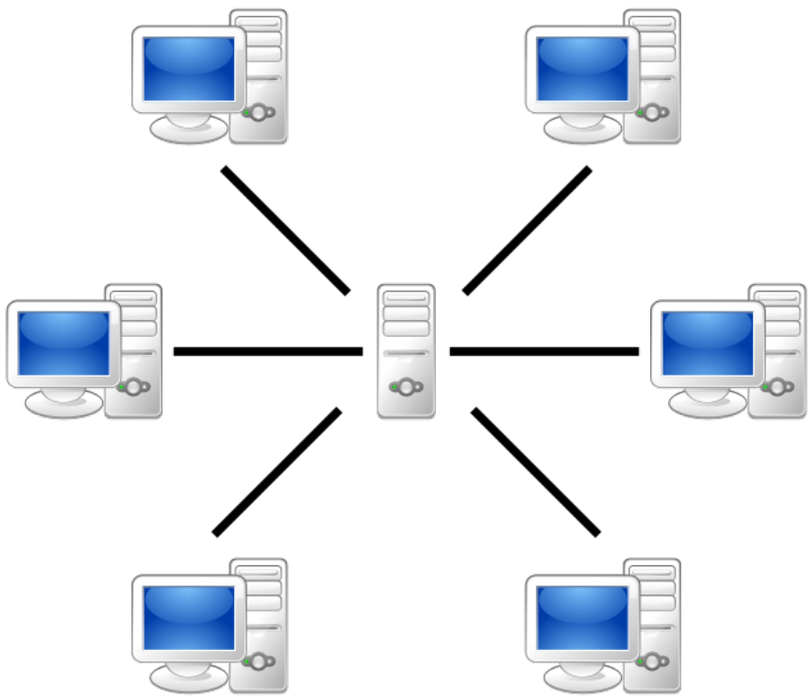


对等网络(Peer-to-Peer)

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







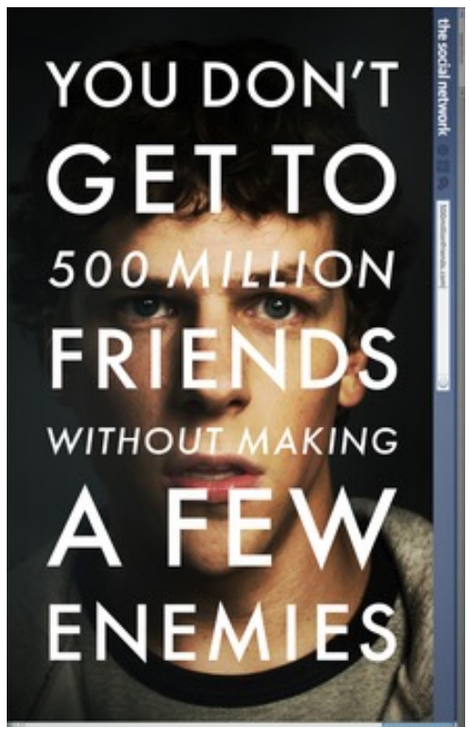
Peer to Peer

napster™

1999

Sean Parker

facebook

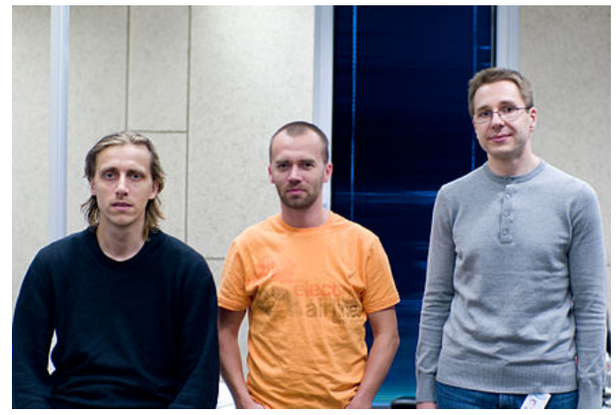


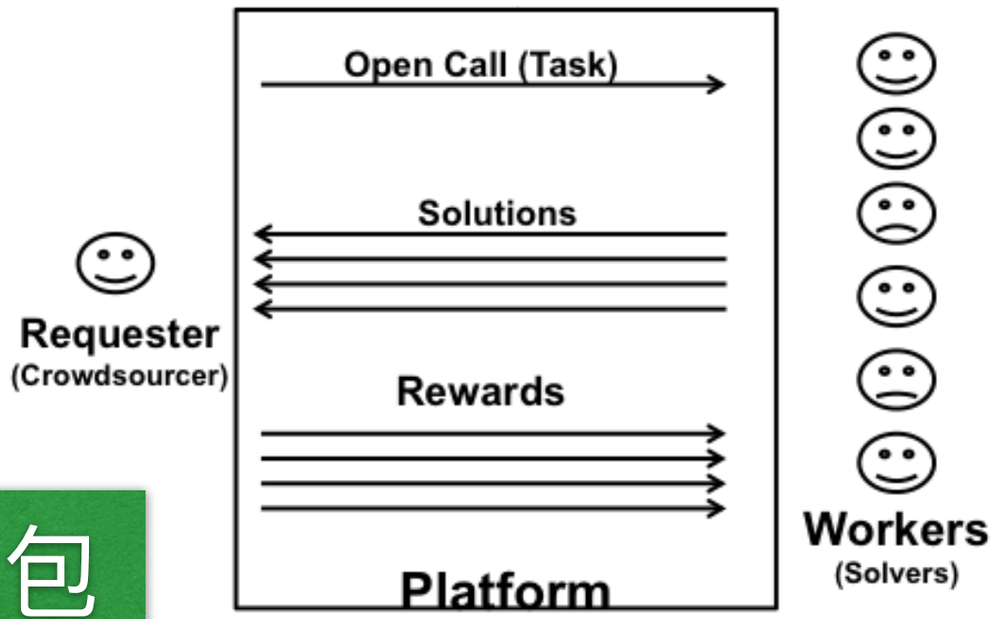
The Social Network

skype™

2003

KaZaA





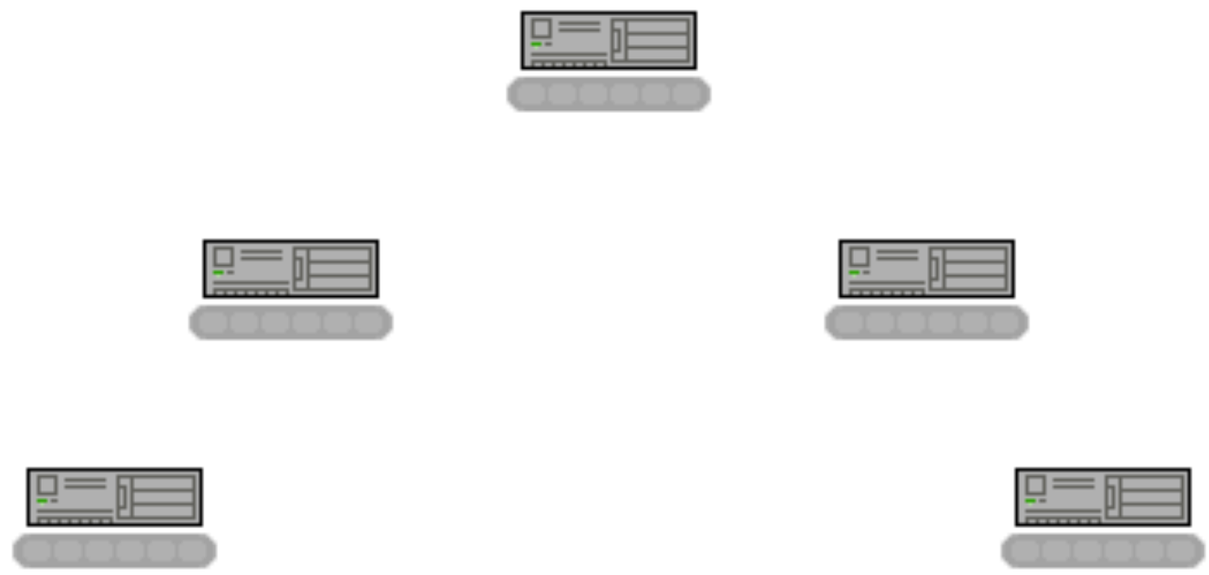
众包

BitTorrent

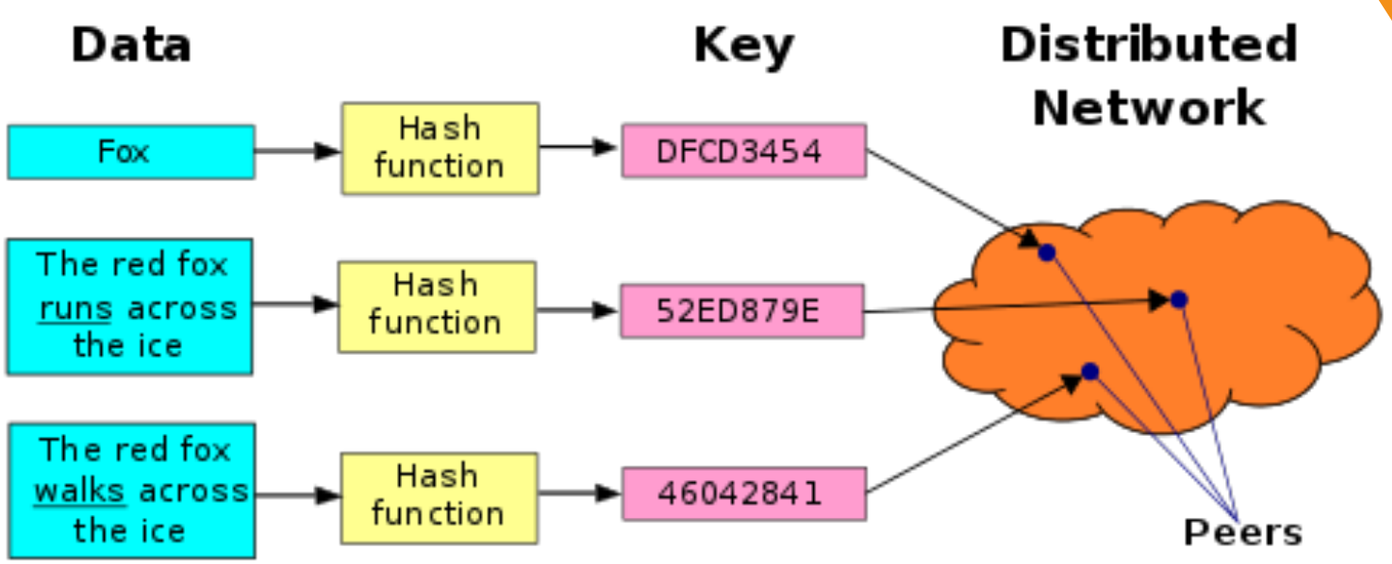
2001

Bram Cohen

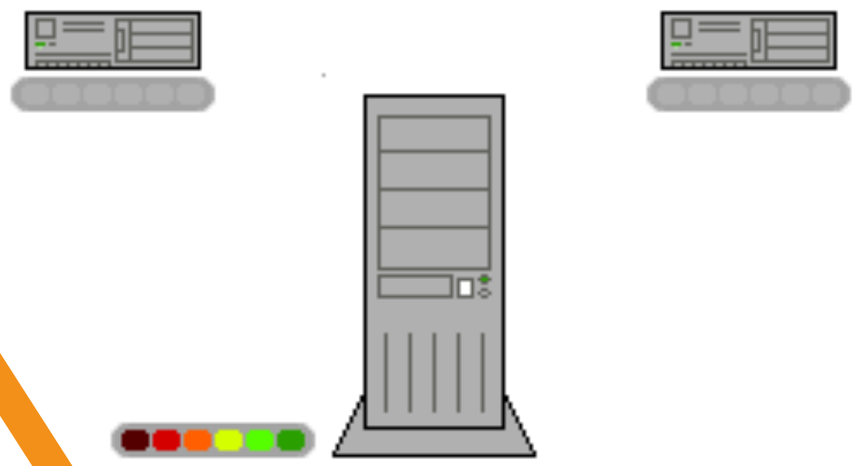
BitTorrent



Distributed Hash Table



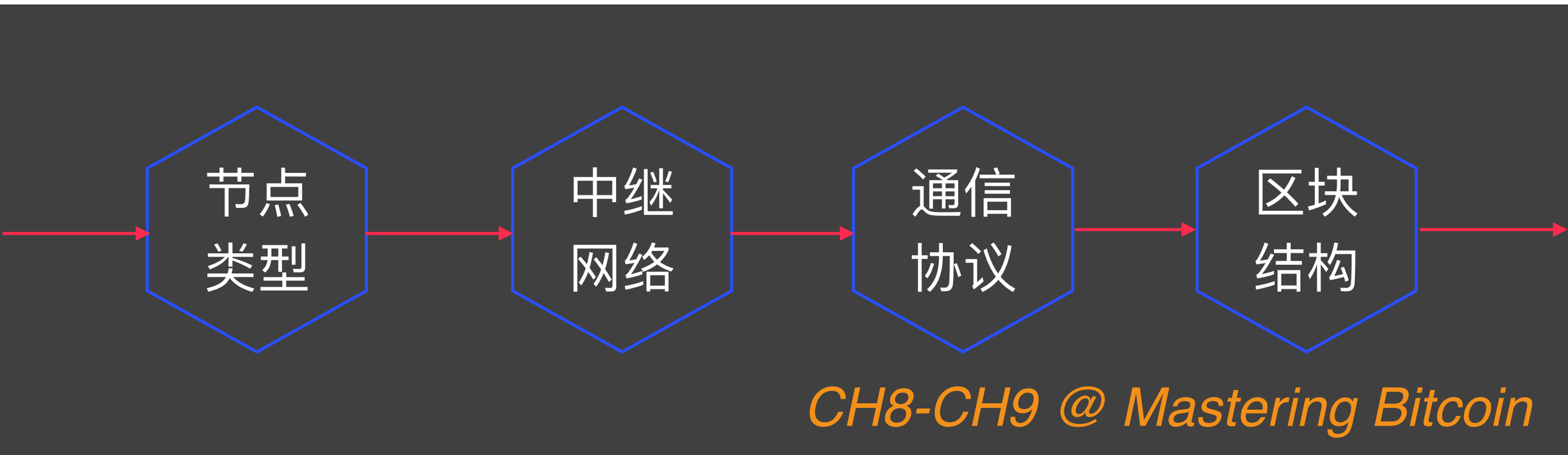
https://en.wikipedia.org/wiki/Distributed_hash_table



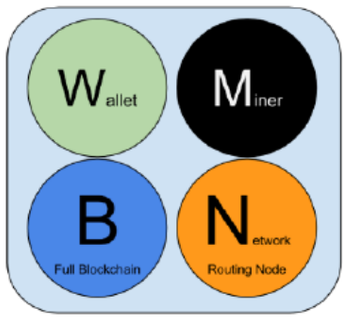
激励

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

网络、区块链

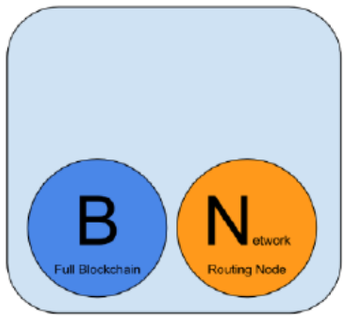


节点类型



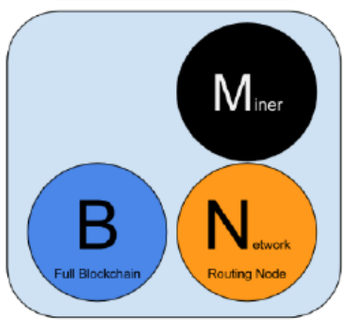
Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



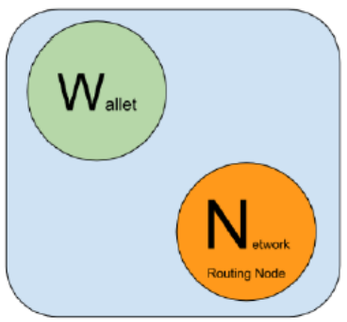
Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



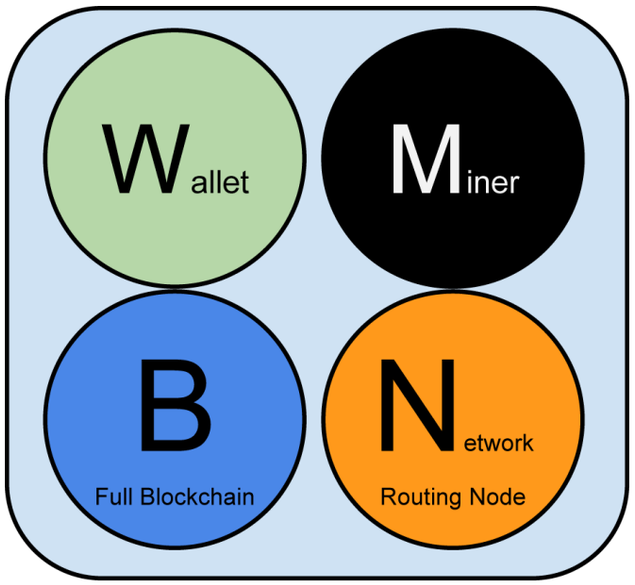
Solo Miner

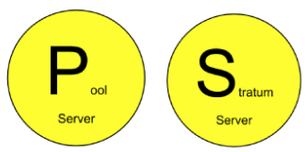
Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



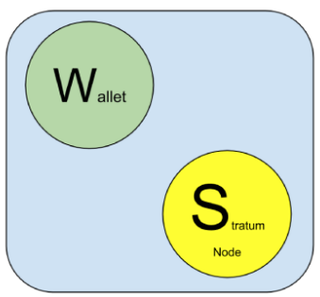


Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.

Mining Nodes

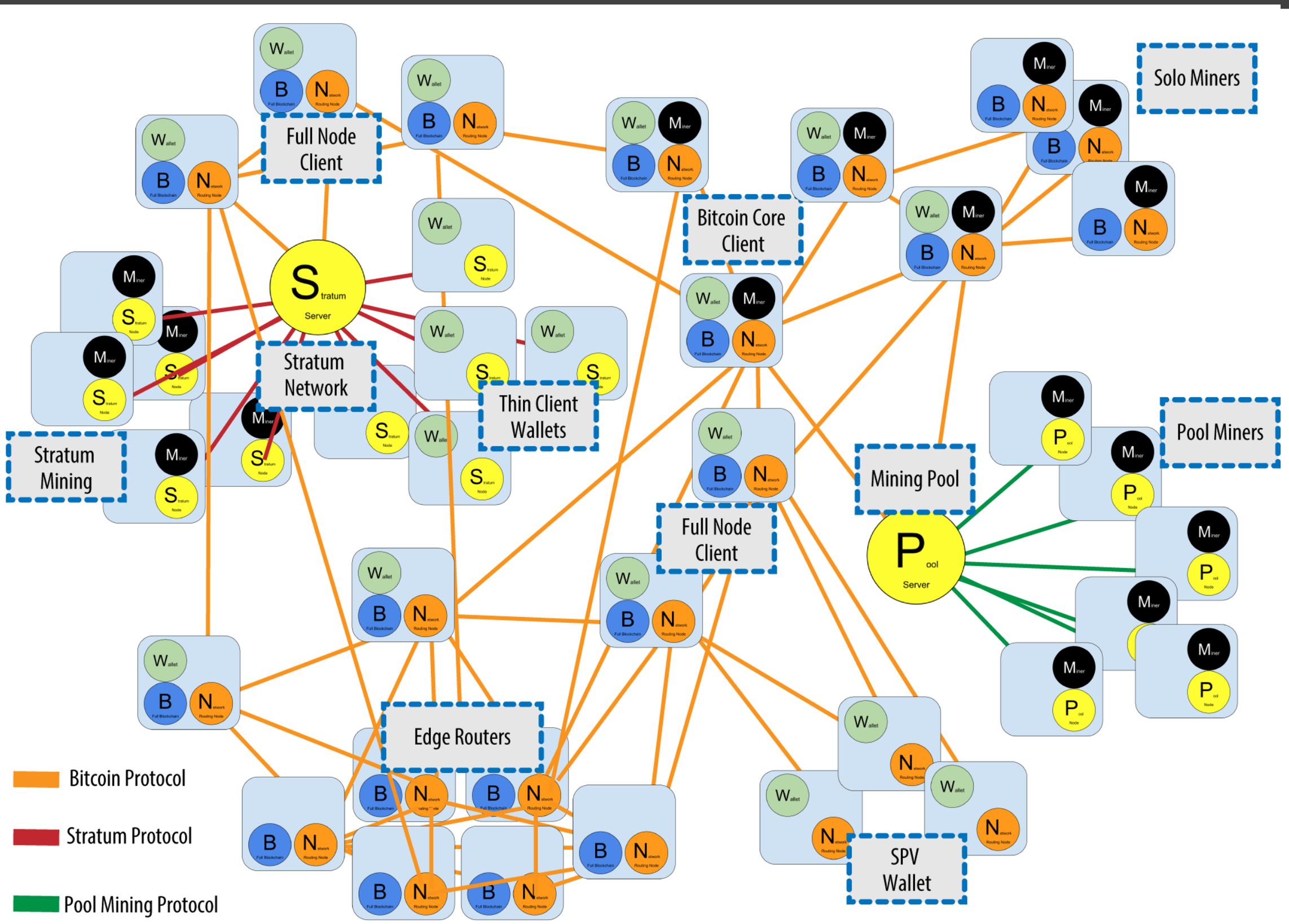
Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



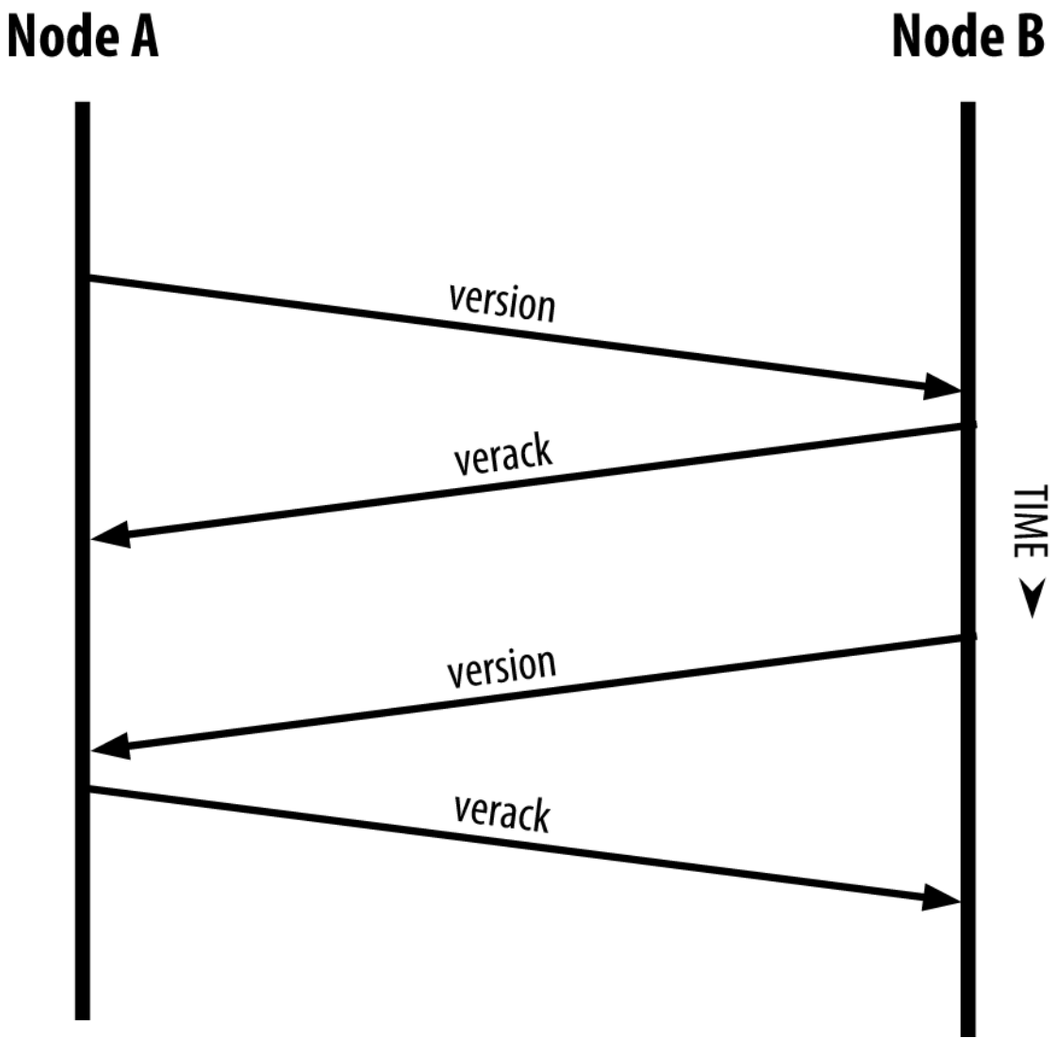
Lightweight (SPV) Stratum wallet

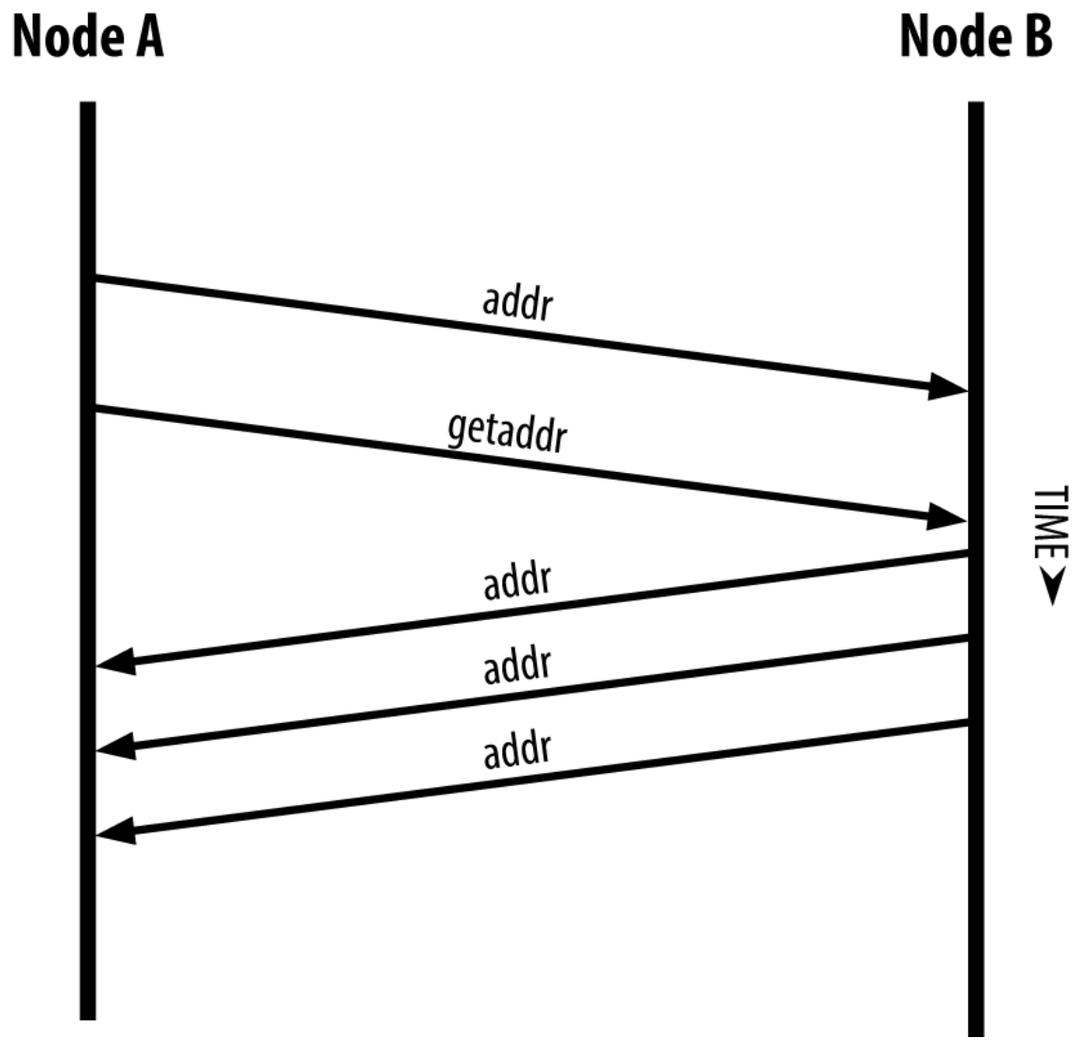
Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

中继网络

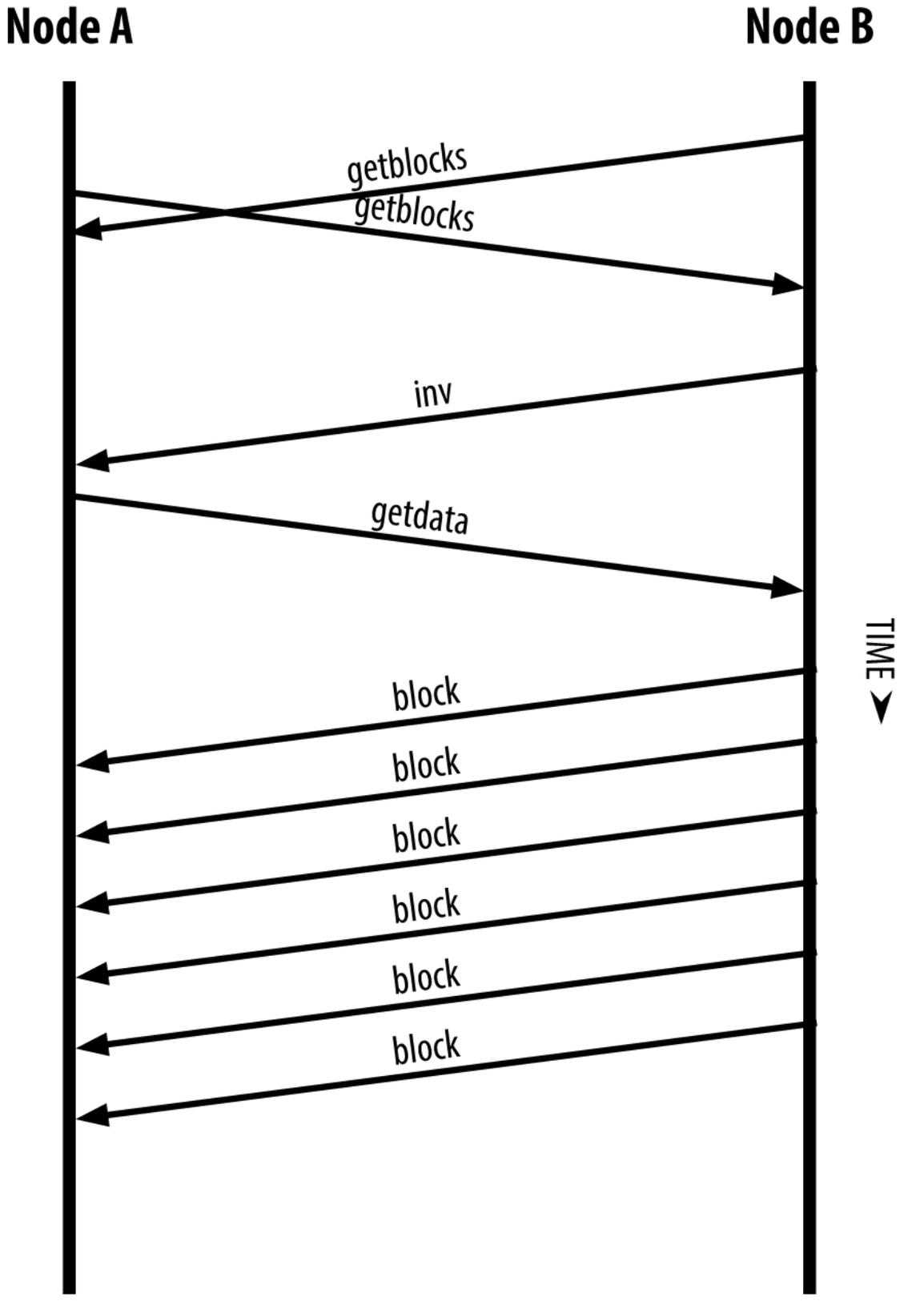

Wallet
B
Full Blockchain
N
Routing Node
Full Node Client
Miner
Solo Miners
Bitcoin Core Client
Stratum Server
Stratum Node
Stratum Network
Thin Client Wallets
Stratum Mining
Pool
Mining Pool
Pool Server
Pool Miners
Edge Routers
SPV Wallet
Bitcoin Protocol
Stratum Protocol
Pool Mining Protocol

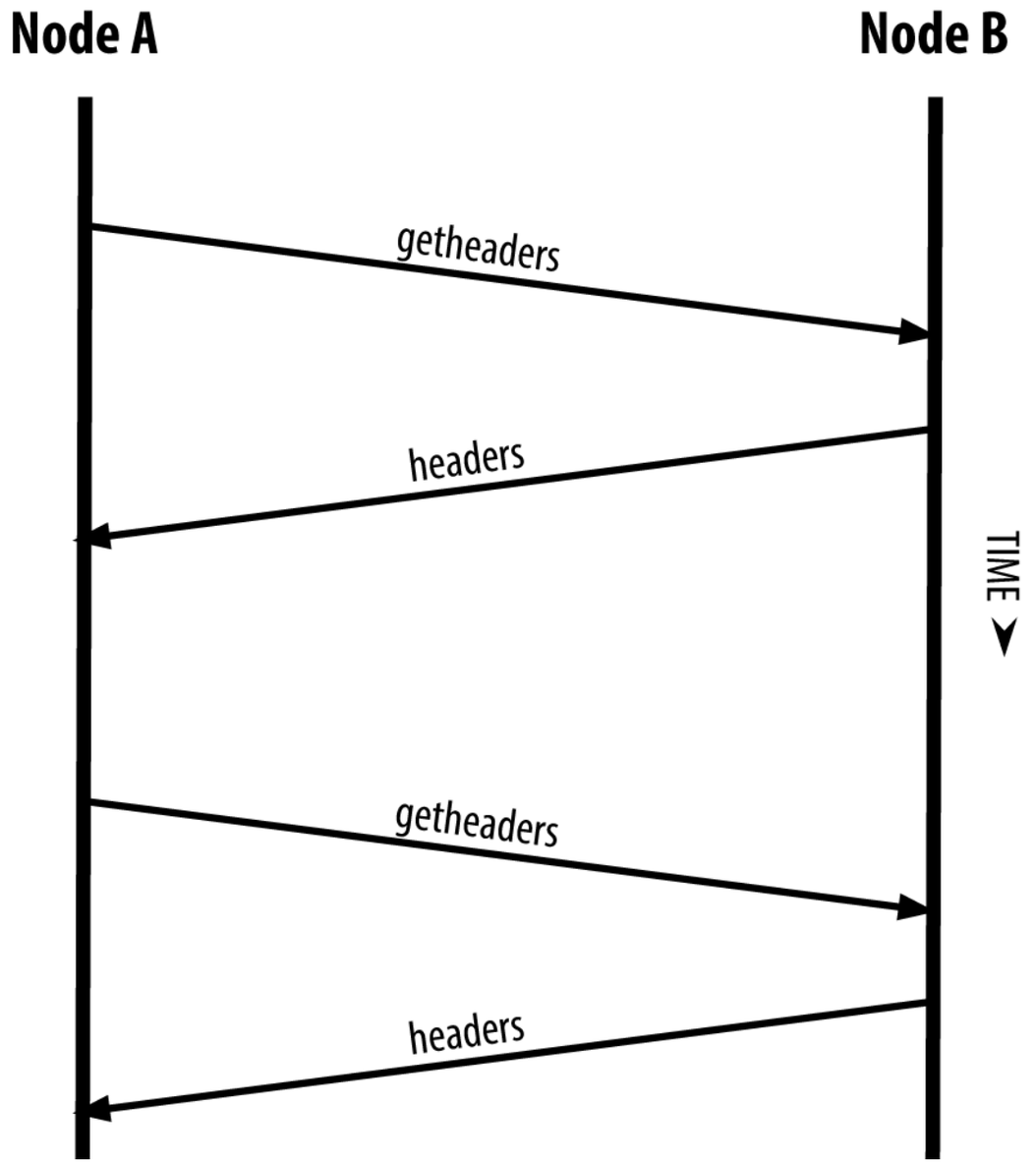
协议


Node A
Node B
version
verack
version
verack
TIME

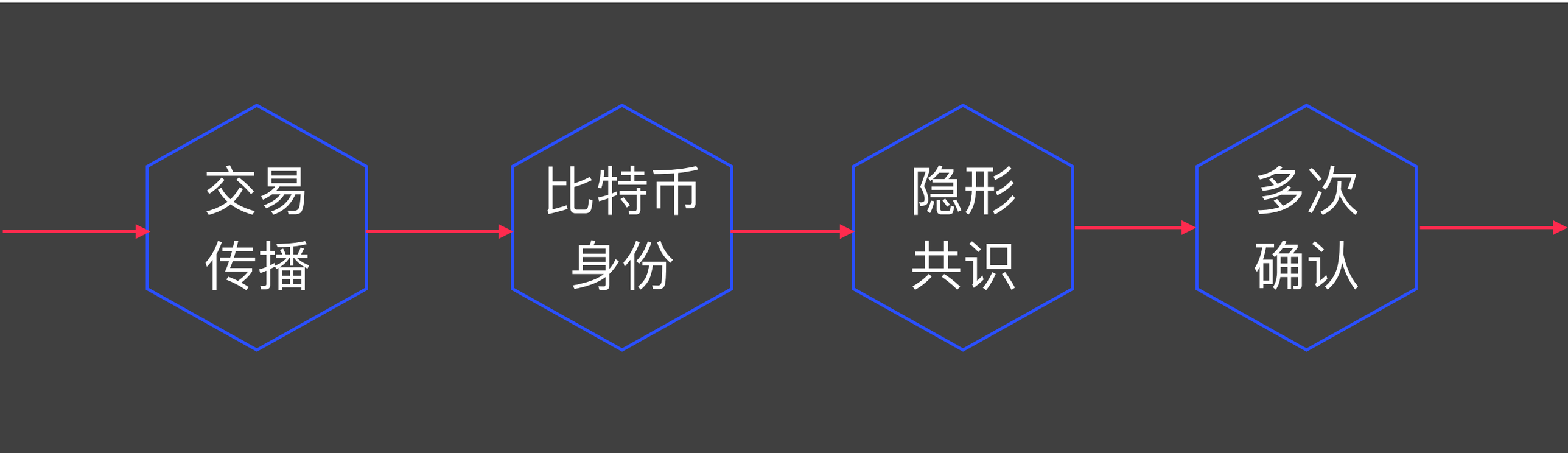

Node A
Node B
addr
getaddr
addr
addr
addr
TIME

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

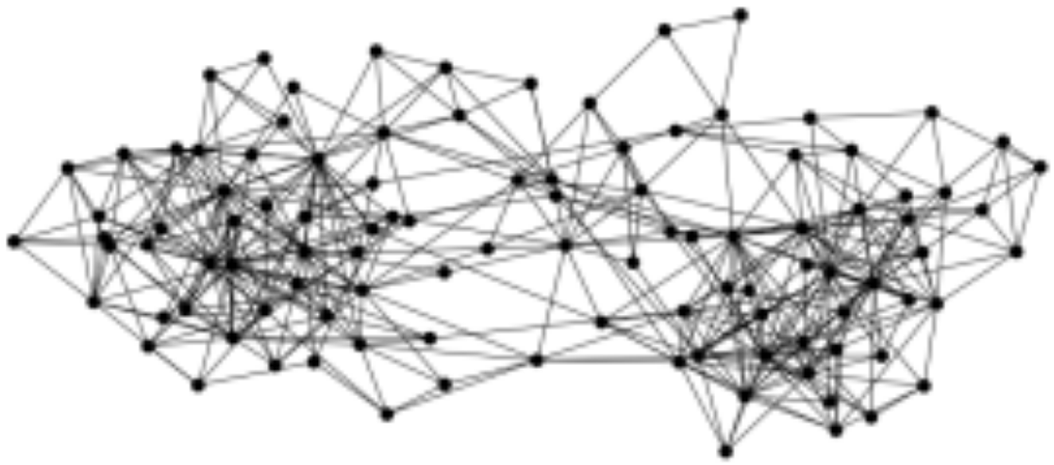
比特币共识



比特币的交易传播

signed by Alice

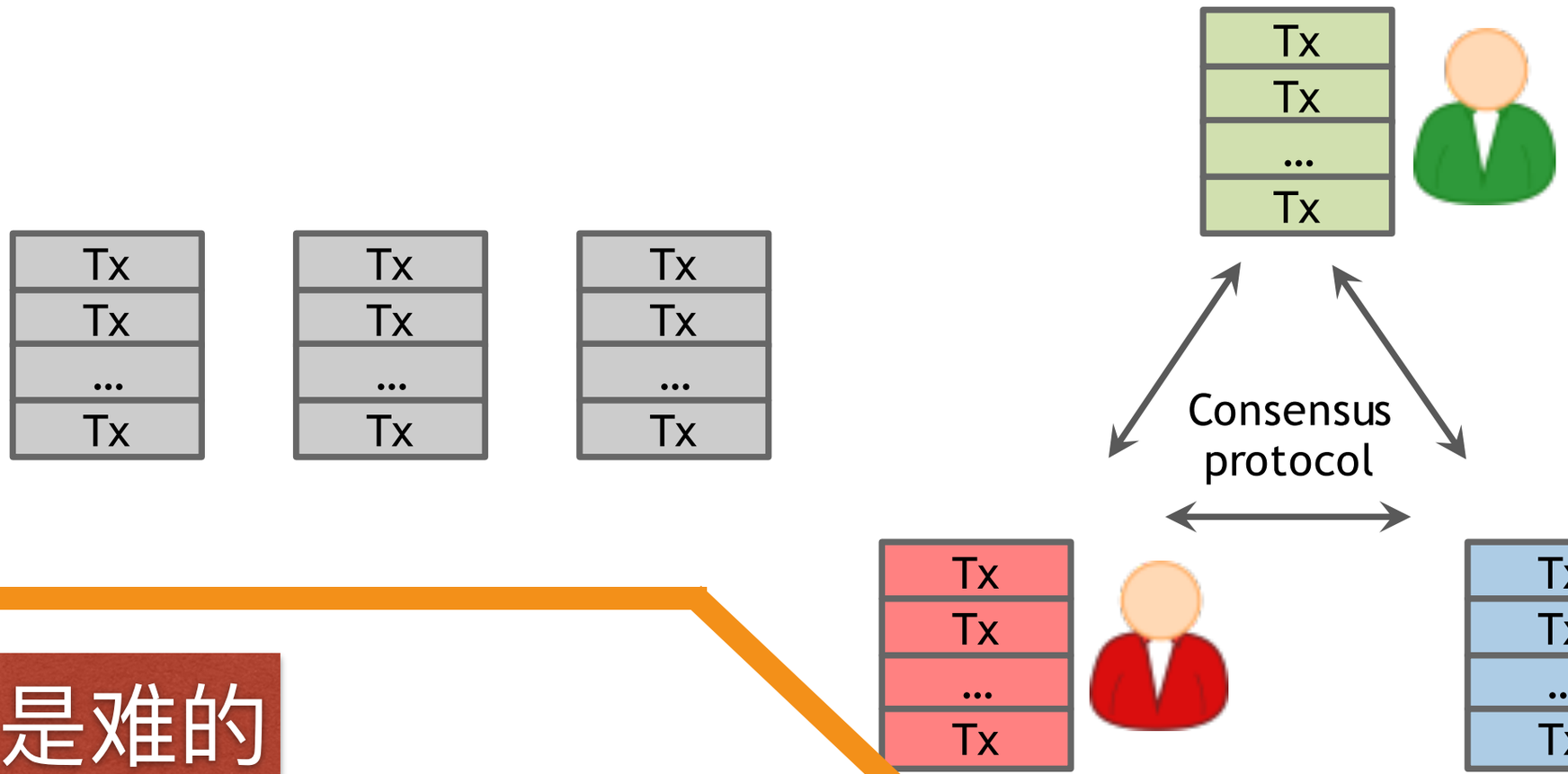
Pay to pk_{Bob} : H( )



- 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)***

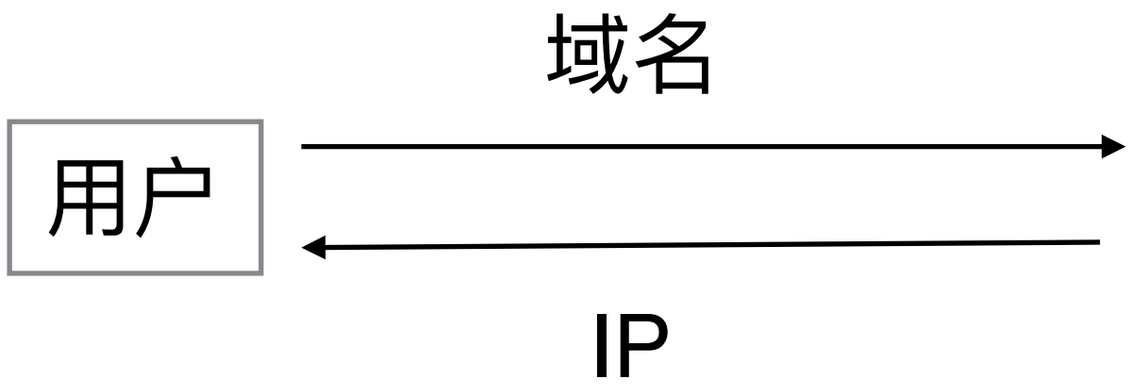
Global Time

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：

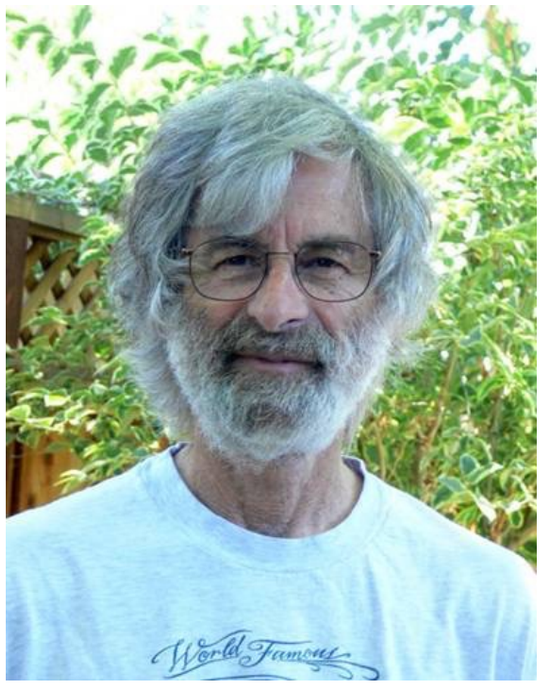
  ✳ 结束时所有诚实的节点均认同该值；

  ✳ 该值由诚实节点产生



Distributed DB, Email, PKI

拜占庭将军问题和Paxos



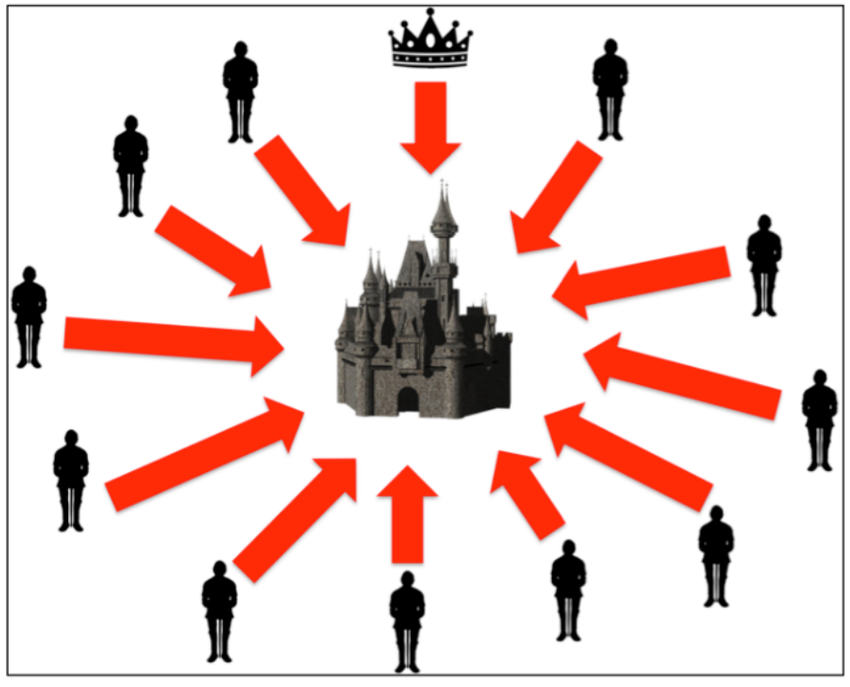
LESLIE LAMPORT

2013图灵奖

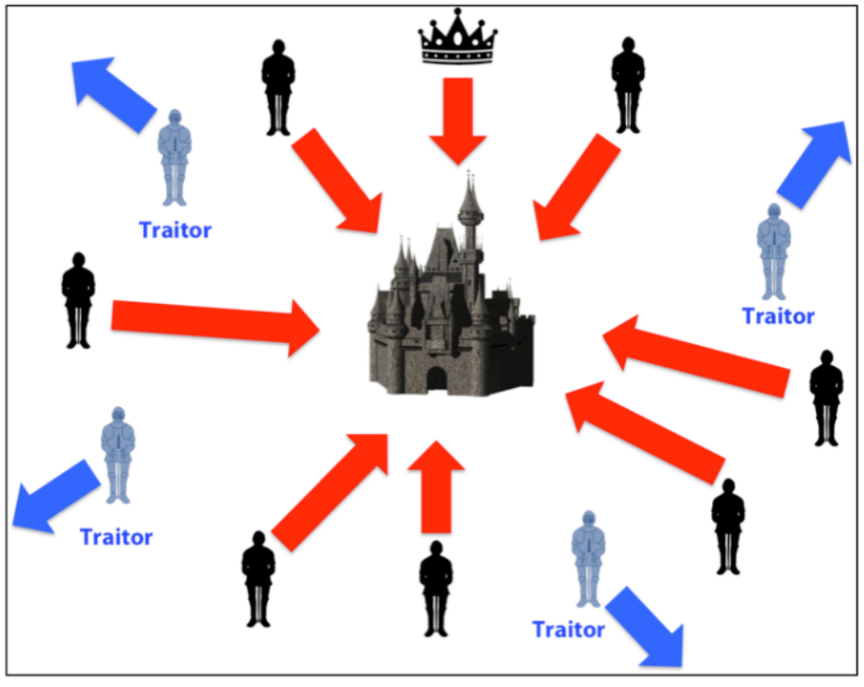
The Byzantine Generals Problem

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

恶意节点

窃取比特币

拒绝服务攻击

双重支付攻击

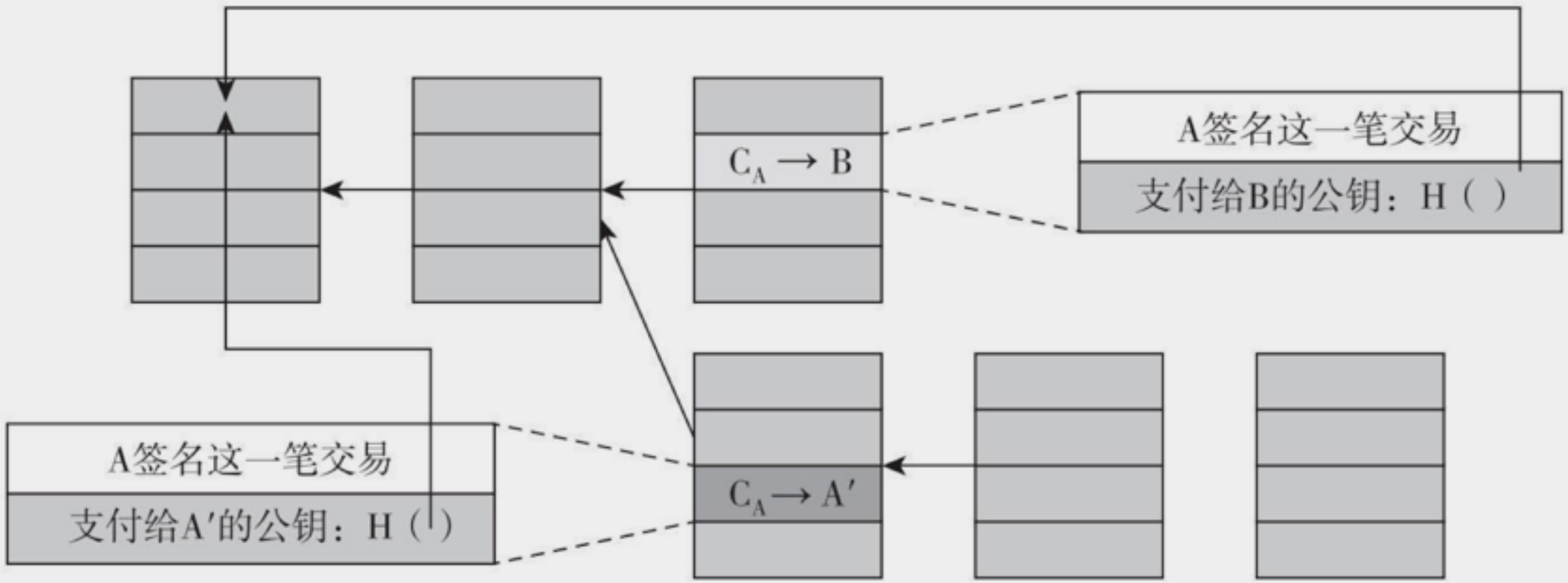


图2.2 双重支付攻击

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

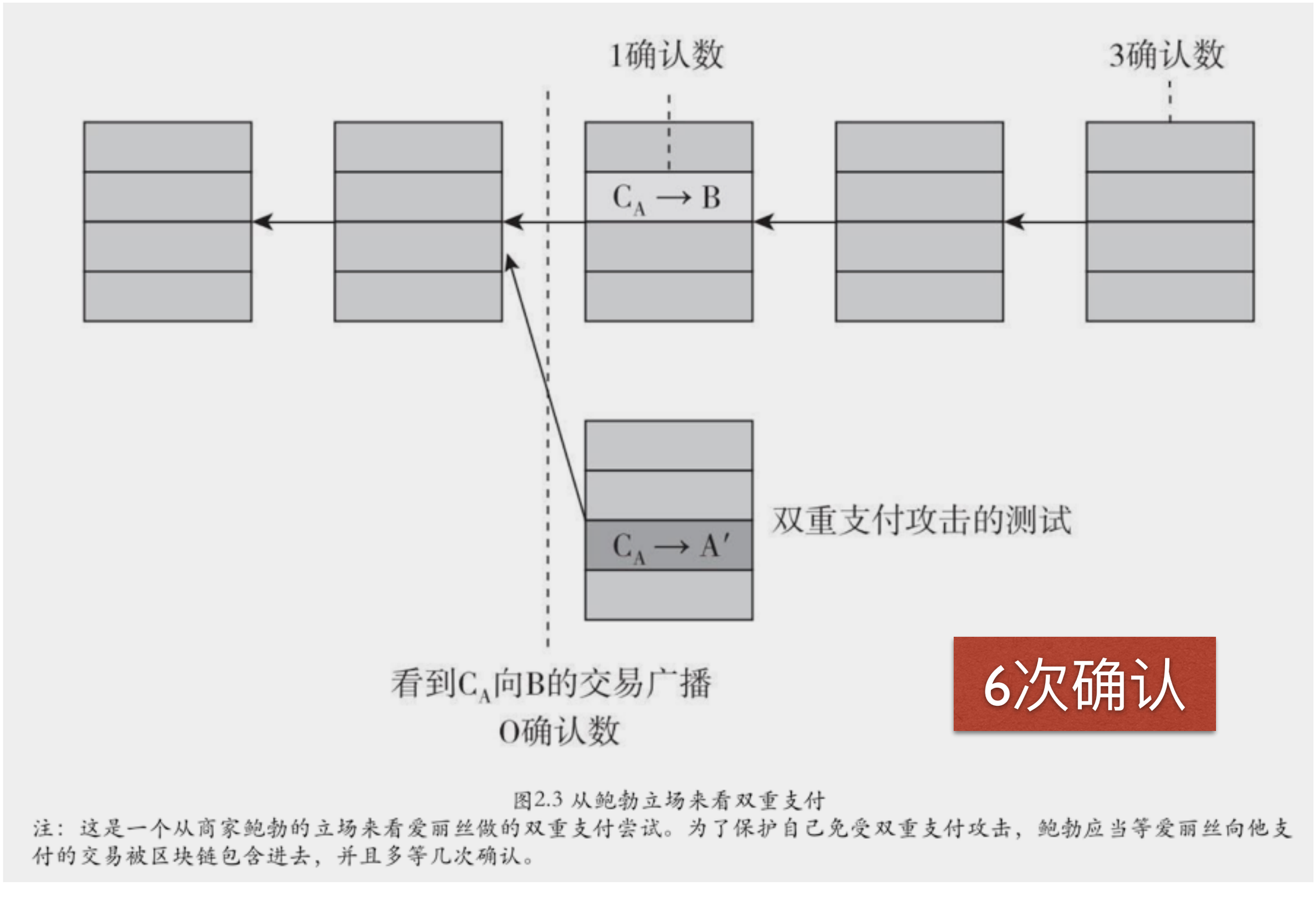
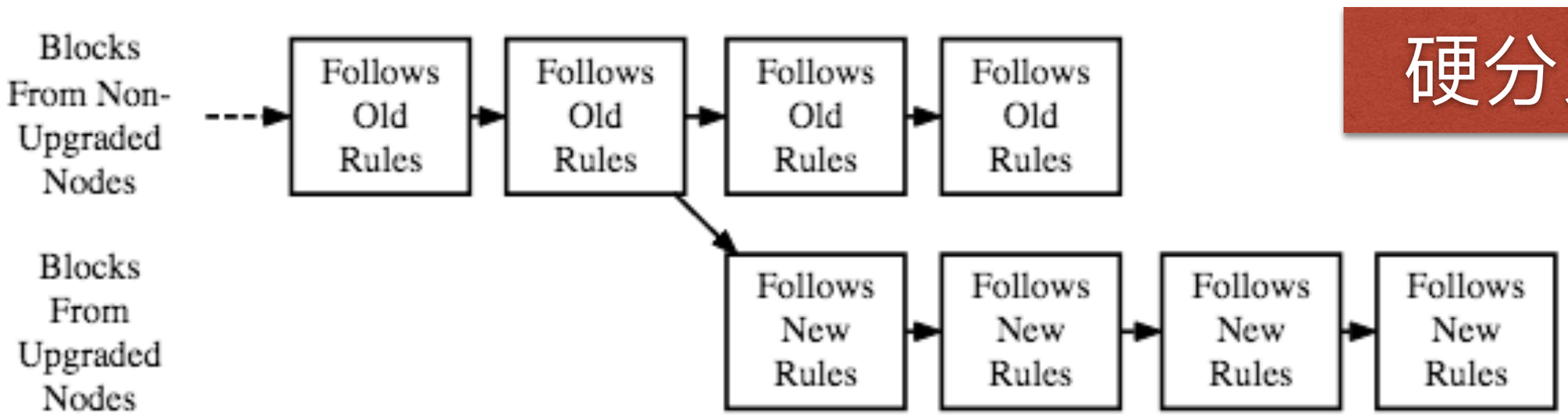


图2.3 从鲍勃立场来看双重支付

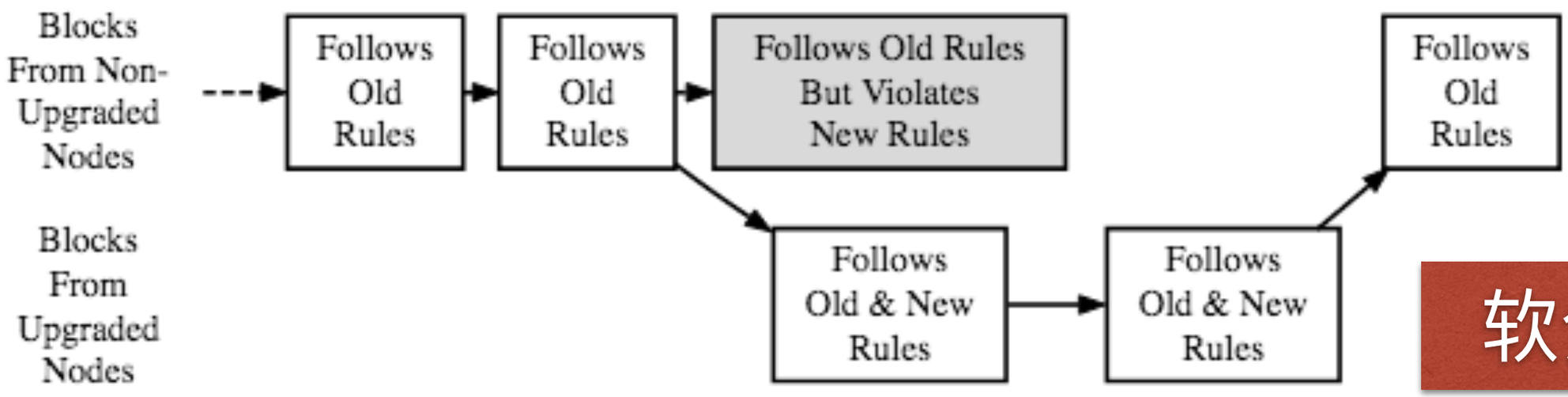
注：这是一个从商家鲍勃的立场来看爱丽丝做的双重支付尝试。为了保护自己免受双重支付攻击，鲍勃应当等爱丽丝向他支付的交易被区块链包含进去，并且多等几次确认。

共识机制改变



硬分叉

A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain



BIP16

BIP30

BIP34

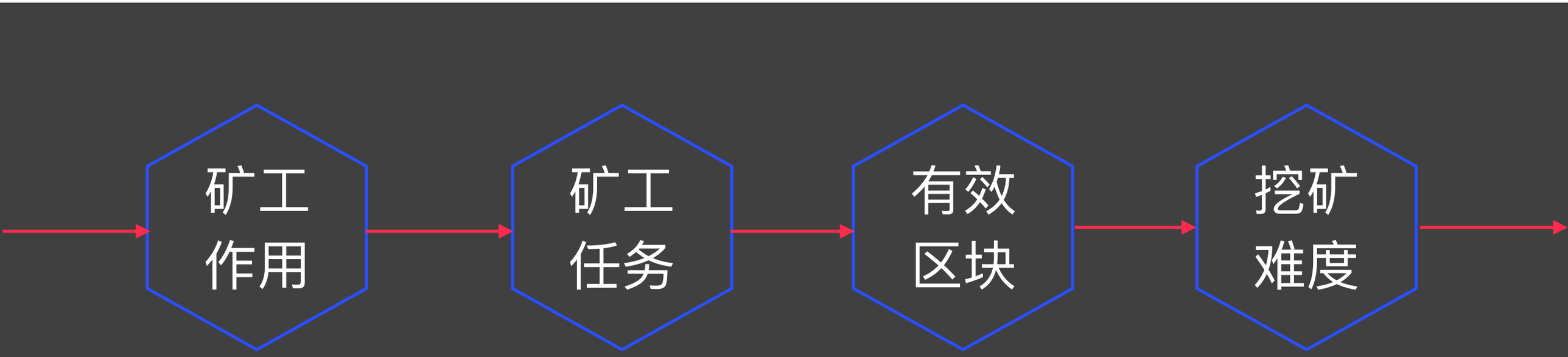
软分叉

A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

比特币的共识总结

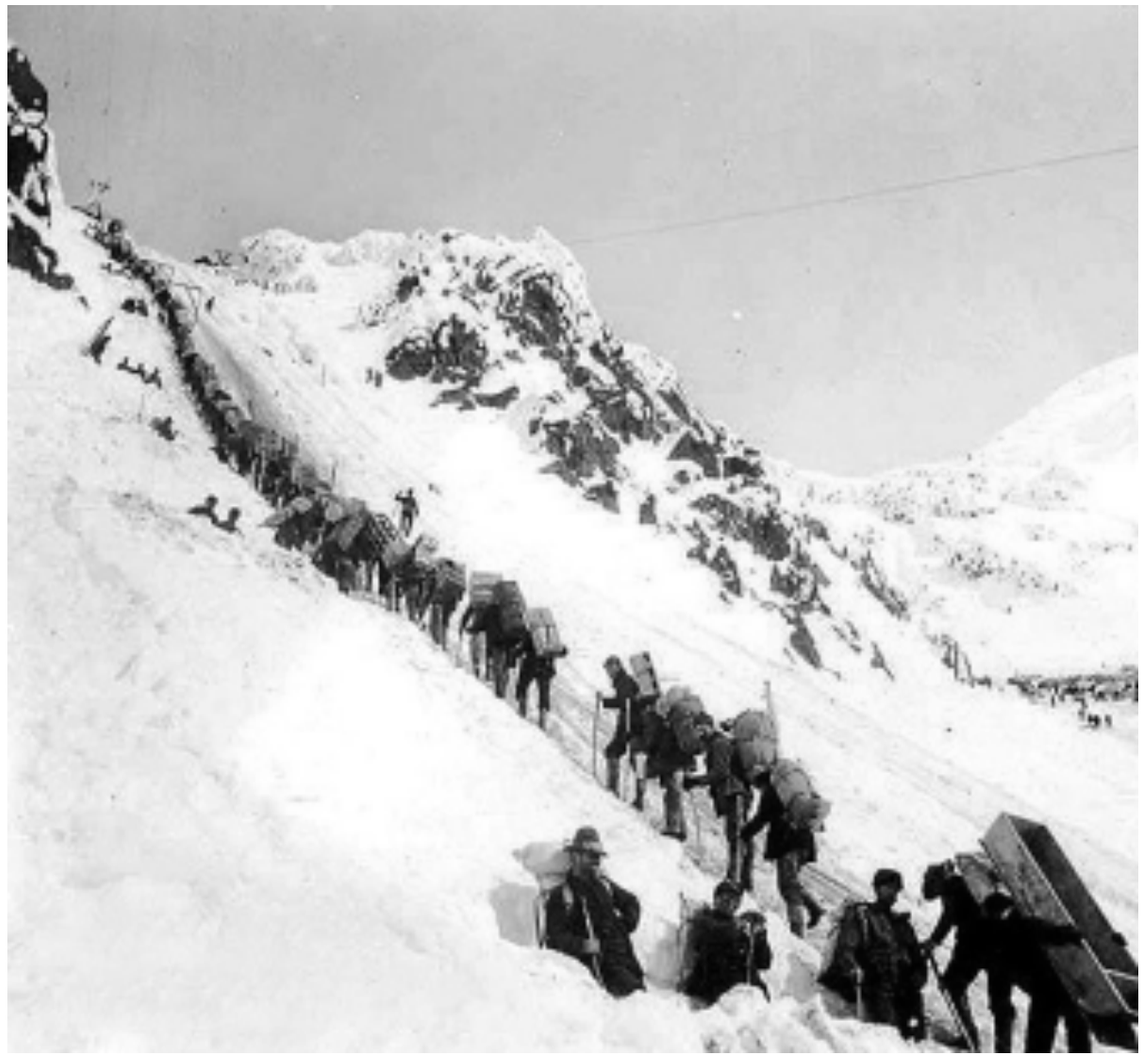
- 理论落后于实践
- 引入了*Incentive*
  - ✳ 是电子货币
- 利用了随机性
  - ✳ 很长时间后才取得共识，*1*小时
  - ✳ 随着时间的增加，对某一块的共识的概率越来越大

比特币挖矿



矿工

- 比特币需要矿工
  - ✳ 存储和广播区块
  - ✳ 验证交易有效性
  - ✳ 对区块进行共识投票



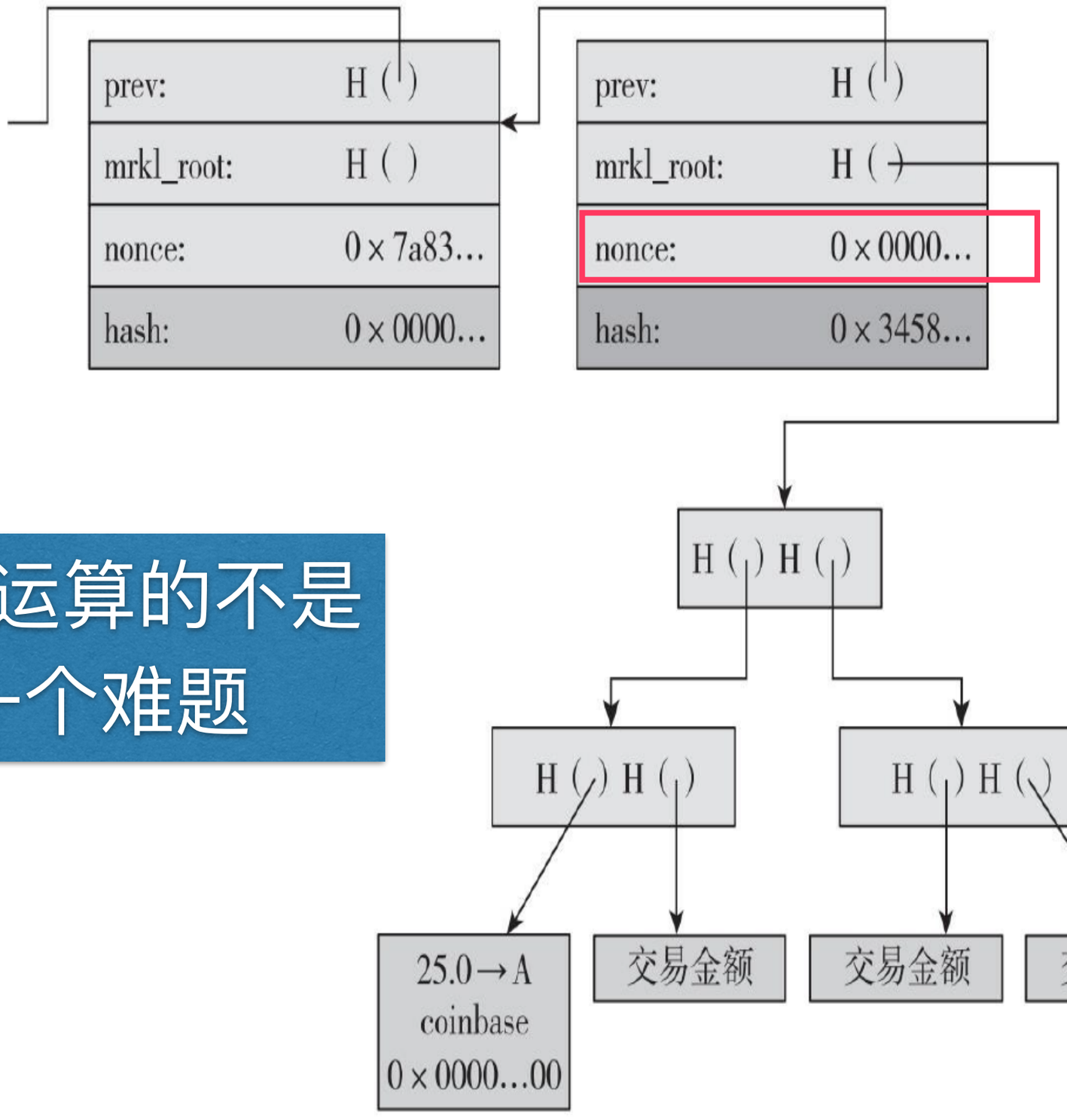
但为什么成为一个矿工！

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

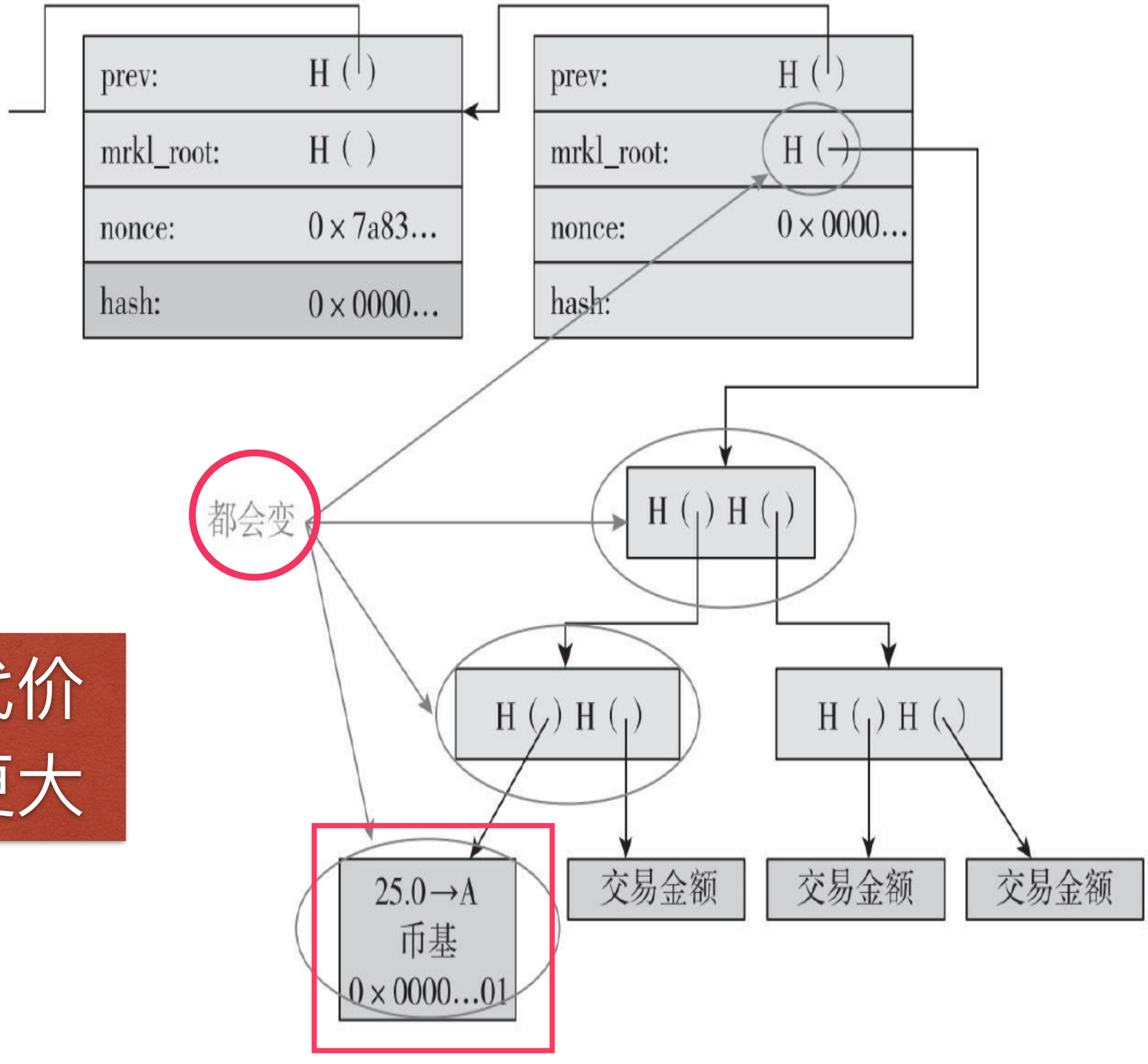
寻找有效区块



32位随机数

每个人运算的不是同一个难题

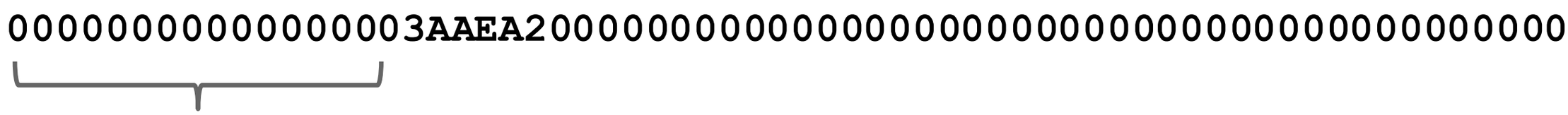
改变临时随机数



代价
更大

挖矿难度

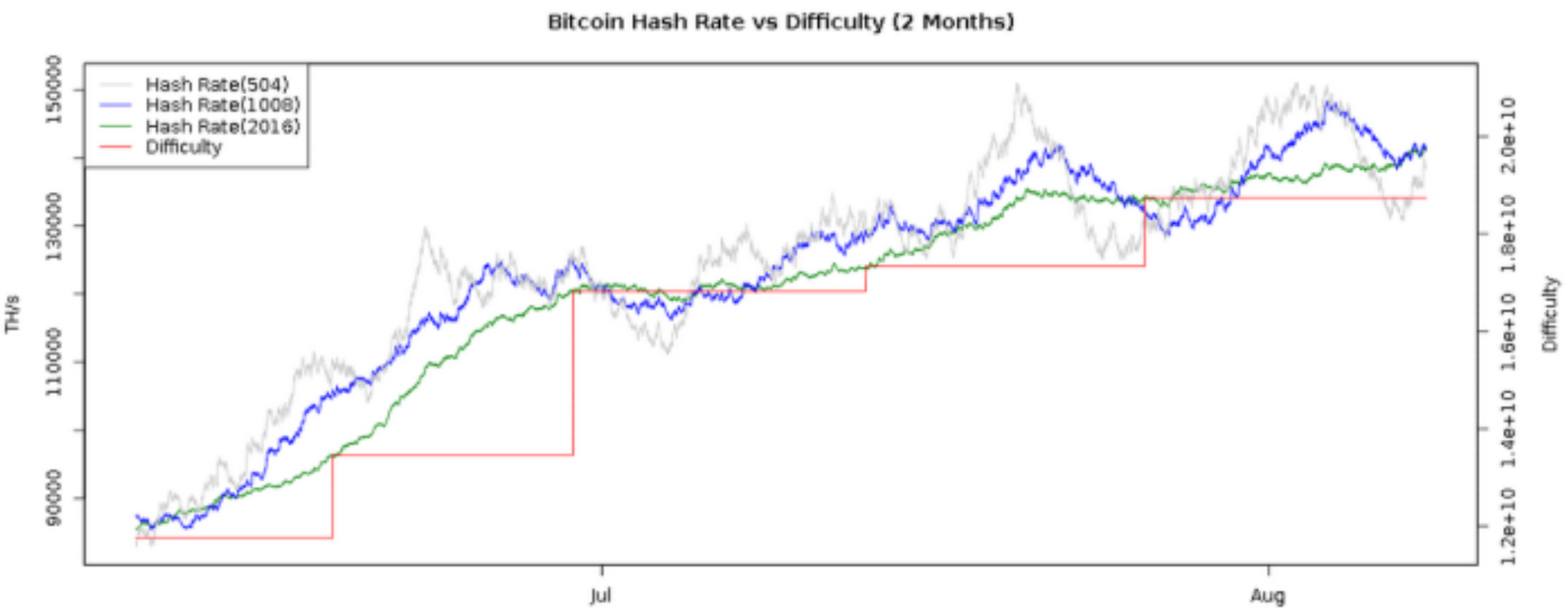
256 bit hash output



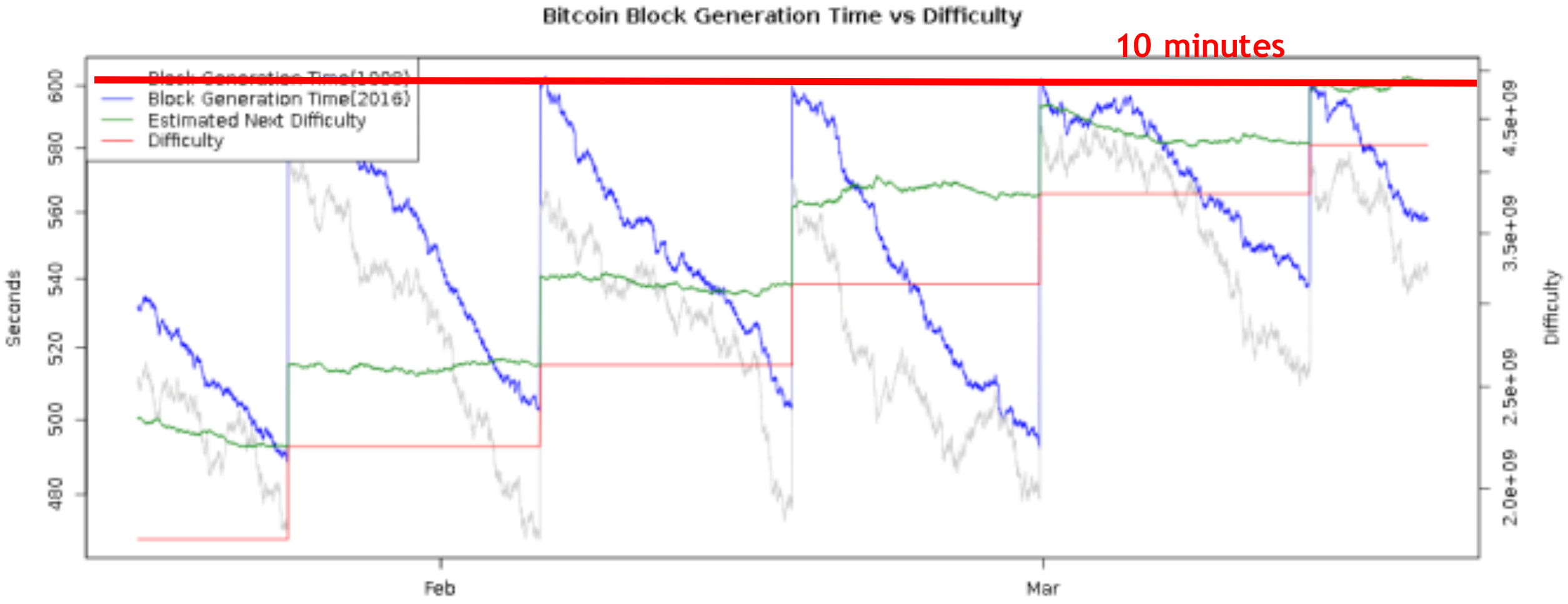
当前难度 = $2^{66.2}$

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

难度随时间变化


Bitcoin Hash Rate vs Difficulty (2 Months)
Hash Rate(504)
Hash Rate(1008)
Hash Rate(2016)
Difficulty
TH/s
150000
130000
110000
90000
Difficulty
2.0e+10
1.8e+10
1.6e+10
1.4e+10
1.2e+10
Jul
Aug

发现一个有效区块的时间



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

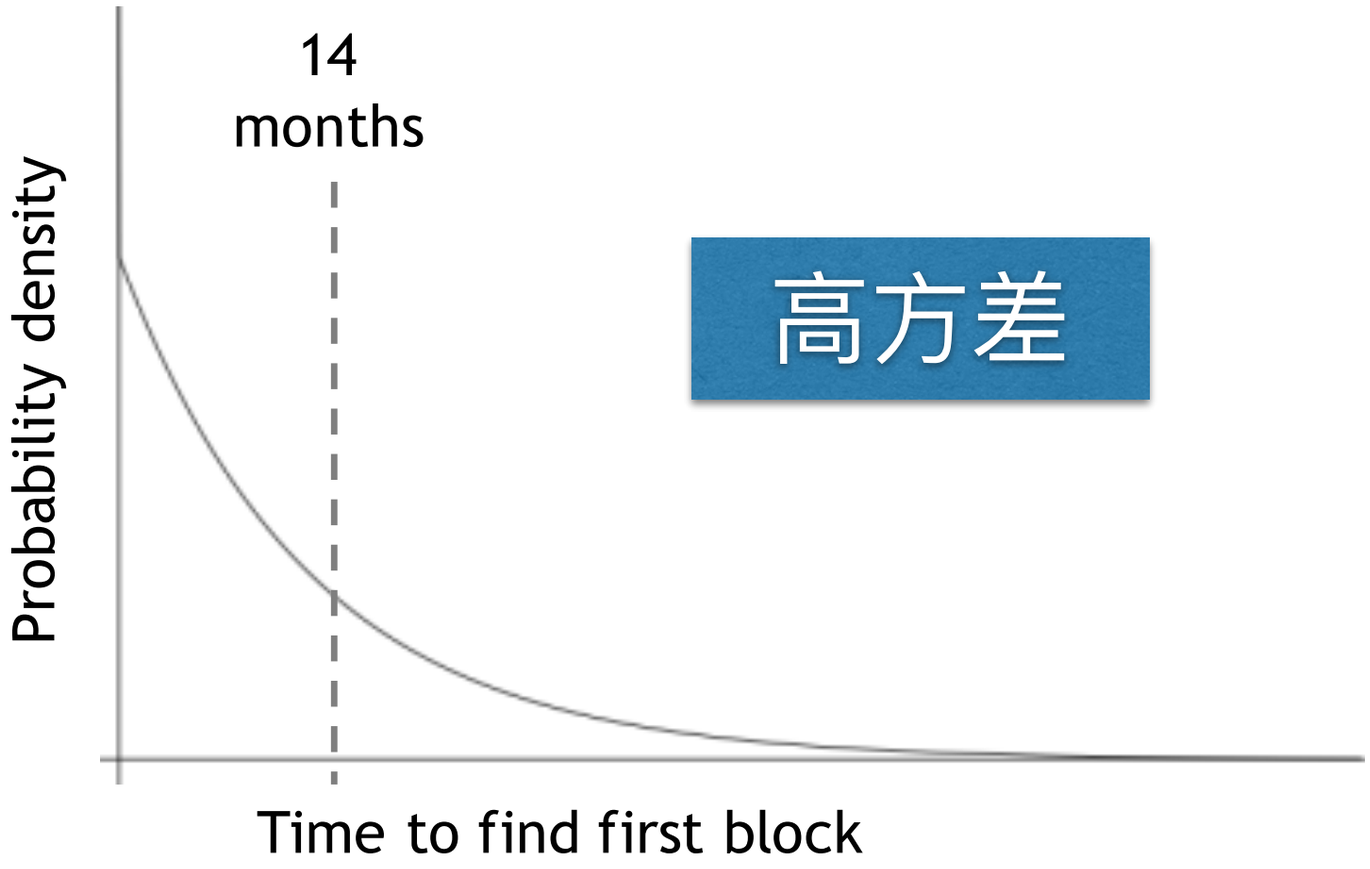
中国

矿池

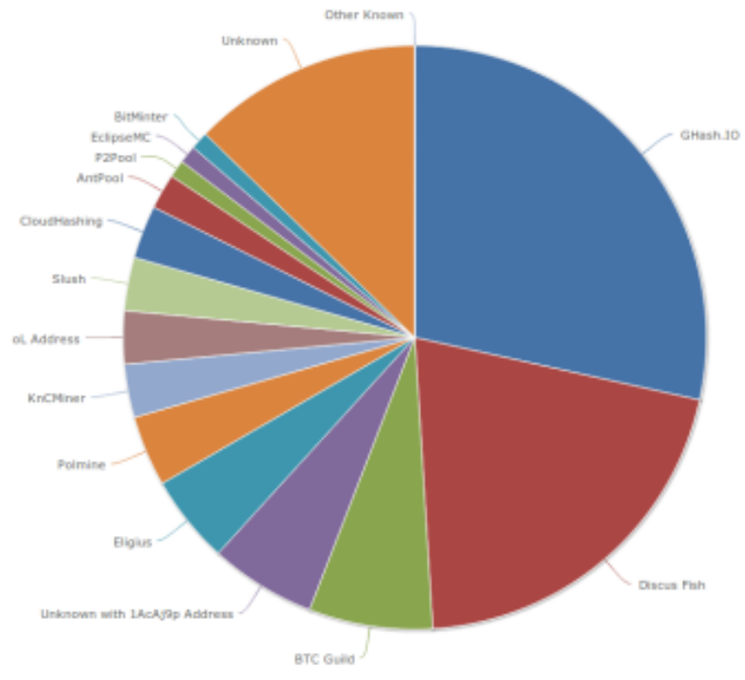
TerraMiner IV

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

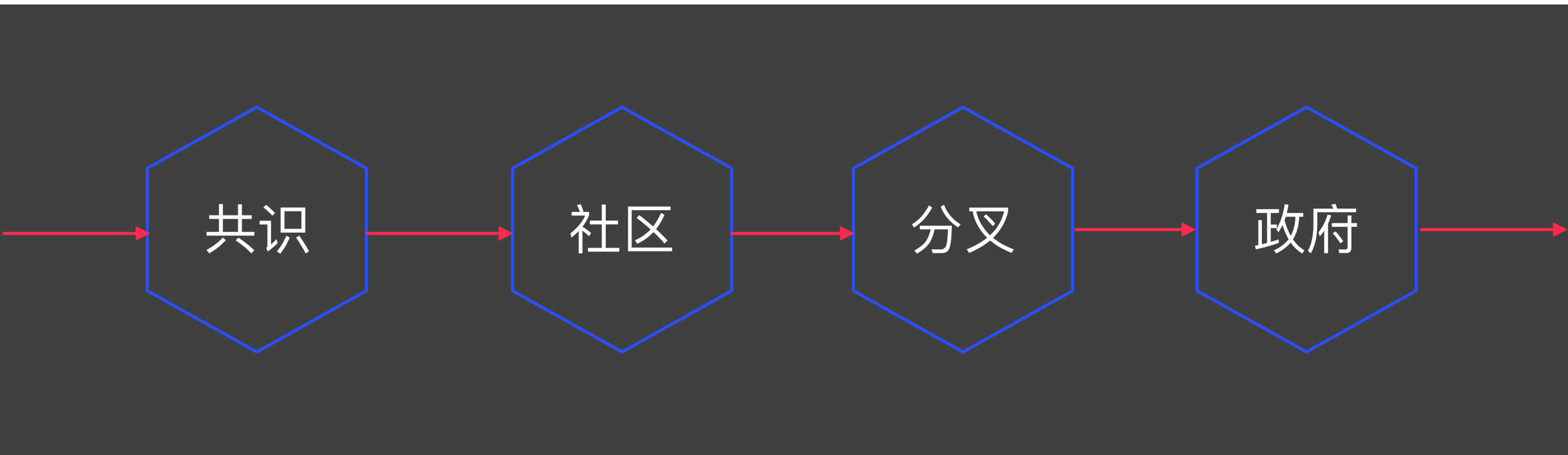
# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%



高方差



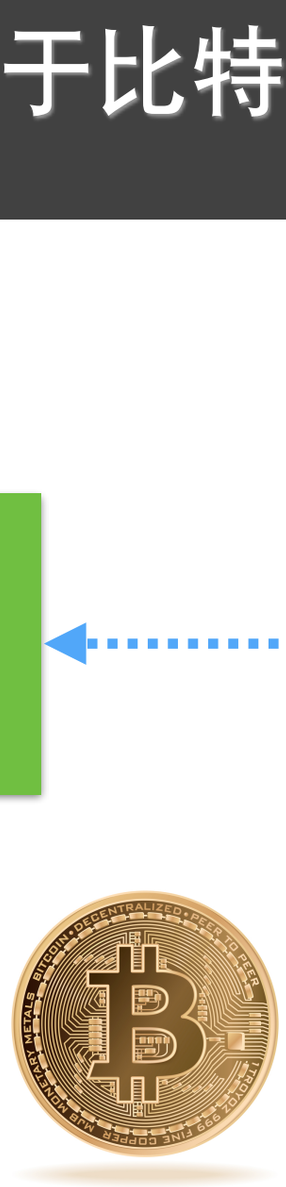
监管



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

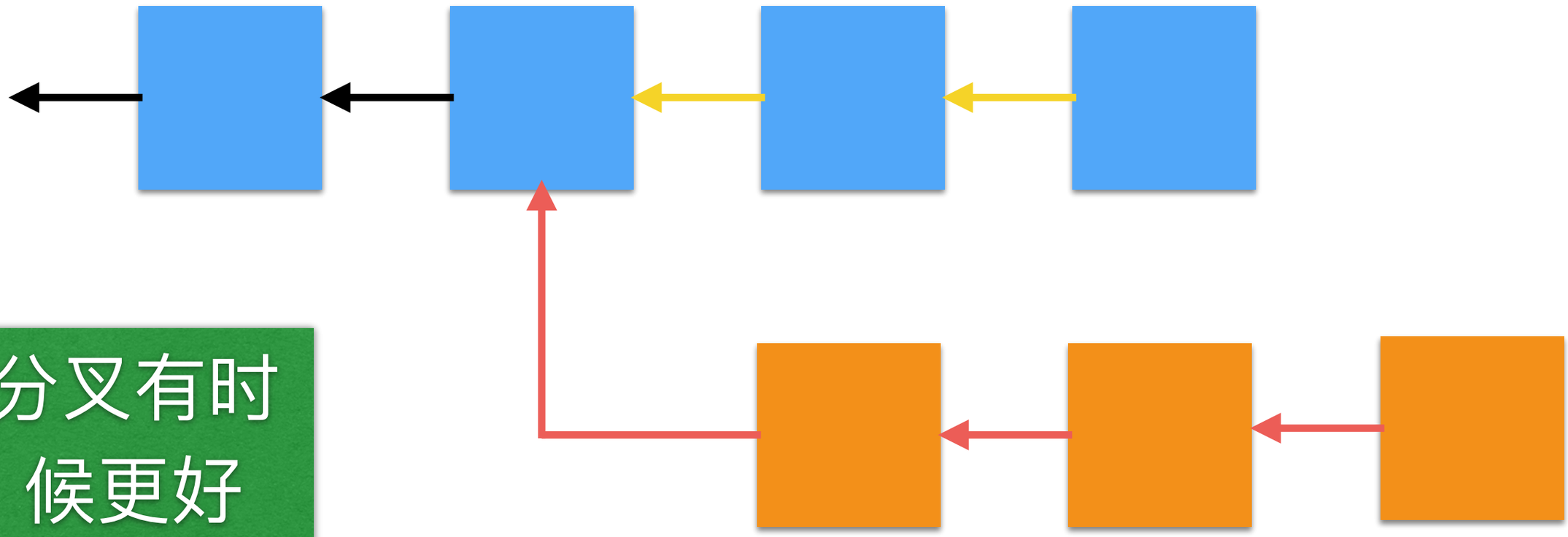
投资人：购买

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

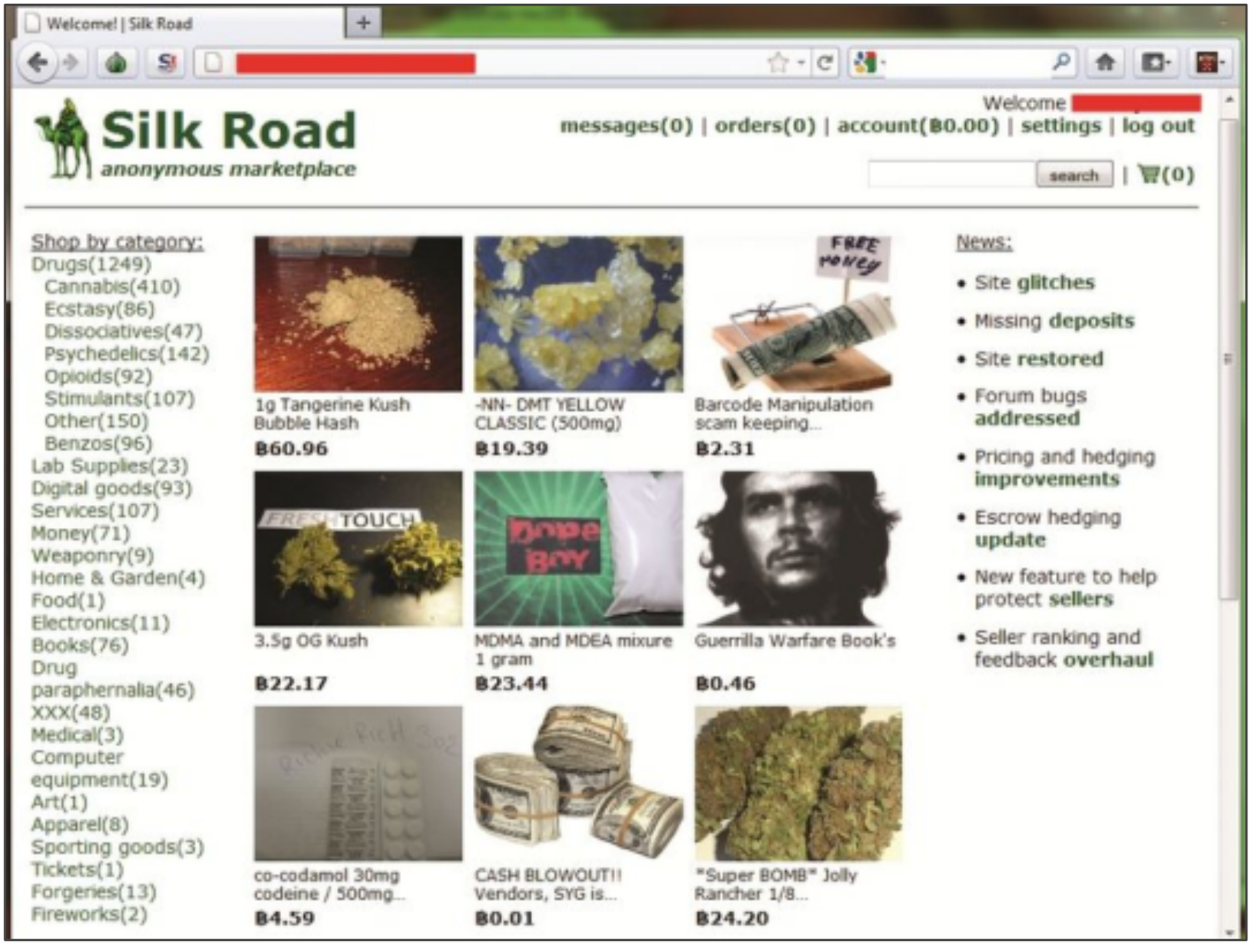
纽约州比特币牌照

美国加密货币管理政策

中国政府2017年系列政策

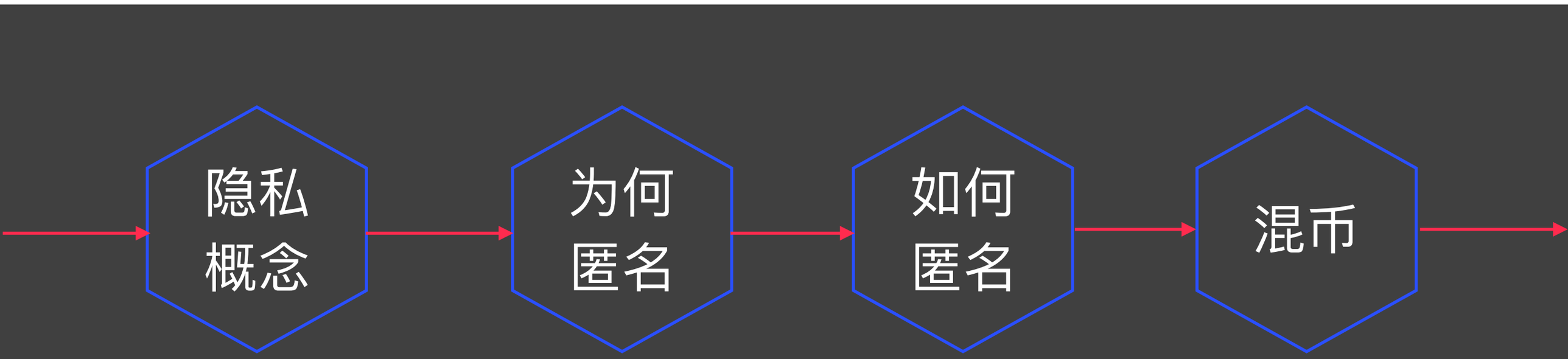
日韩
新加坡

丝绸之路



把现实世界和虚拟世界完全分离开是很困难的

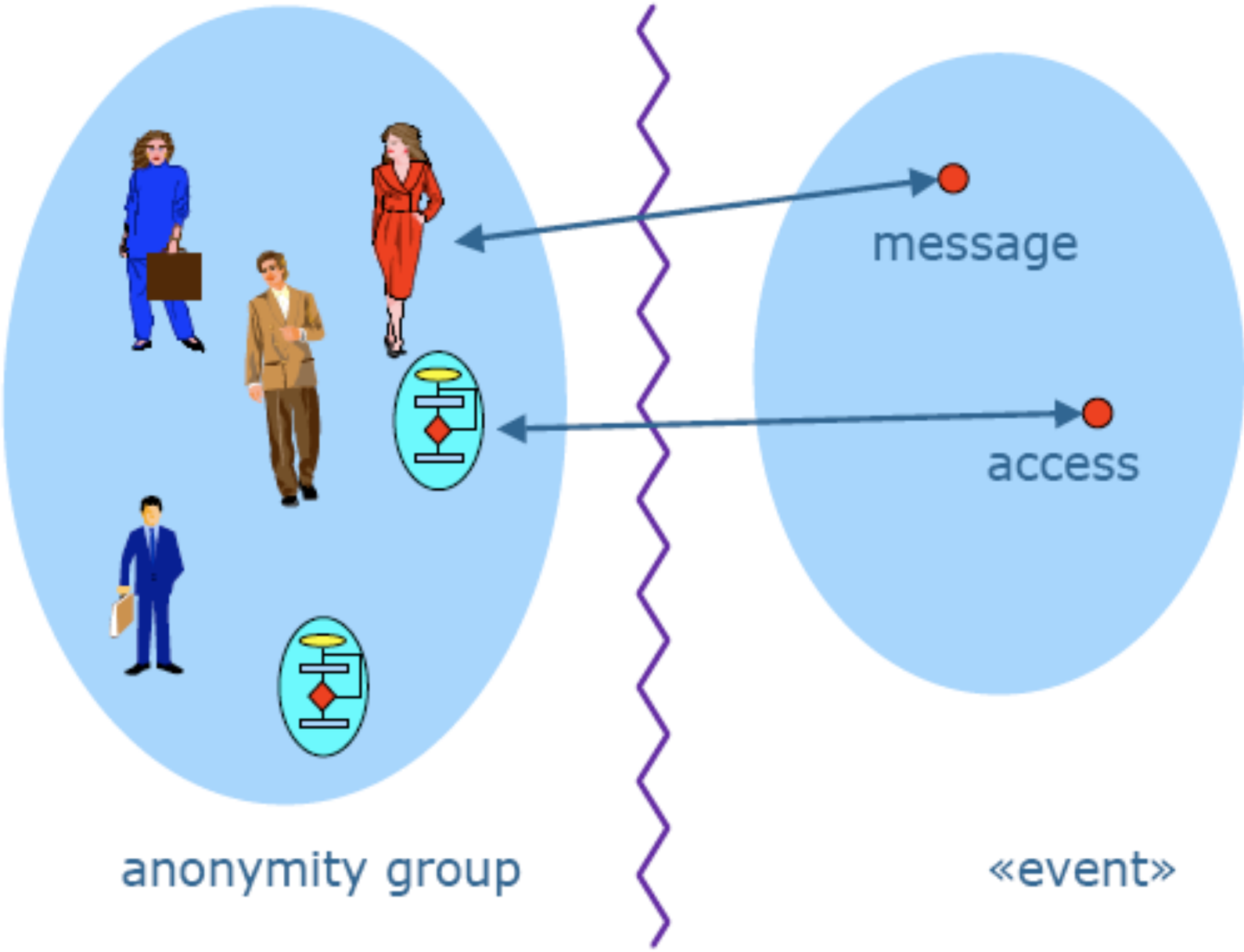
匿名



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

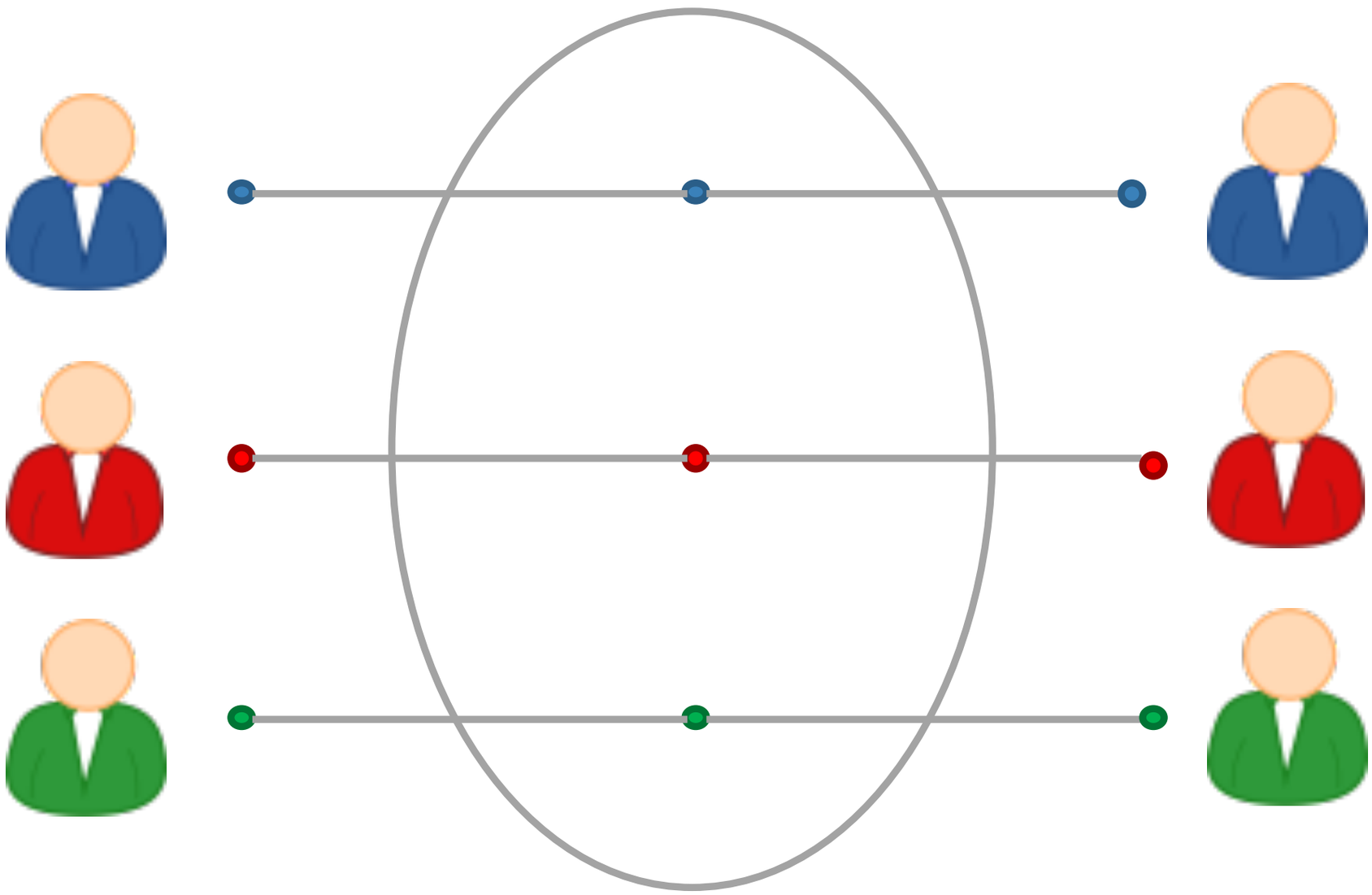
Name	Age	Gender	State of domicile	Religion	Disease
Ramsha	29	Female	Tamil Nadu	Hindu	Cancer
Yadu	24	Female	Kerala	Hindu	Viral infection
Salima	28	Female	Tamil Nadu	Muslim	TB
sunny	27	Male	Karnataka	Parsi	No illness
Joan	24	Female	Kerala	Christian	Heart-related
Bahuksana	23	Male			
Rambha	19	Male			
Kishor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

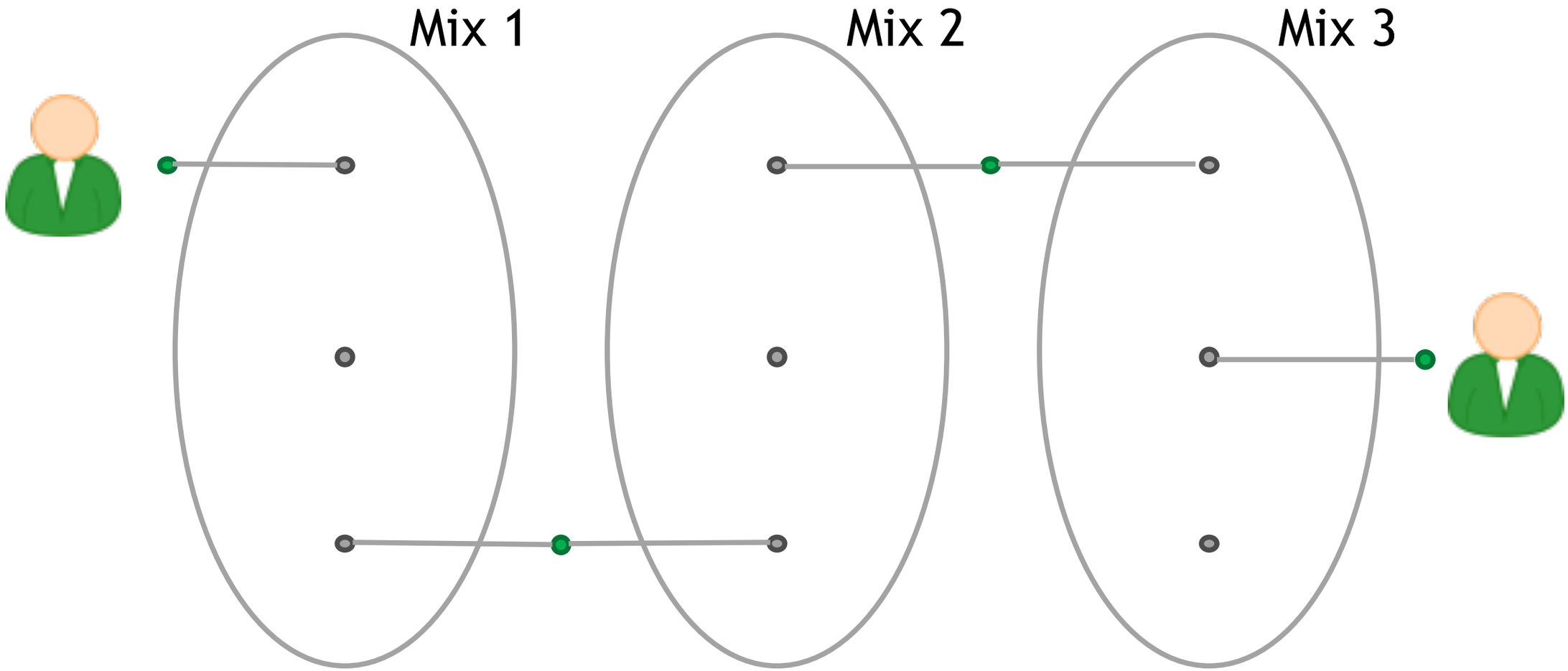


在线钱包

引入中介节点

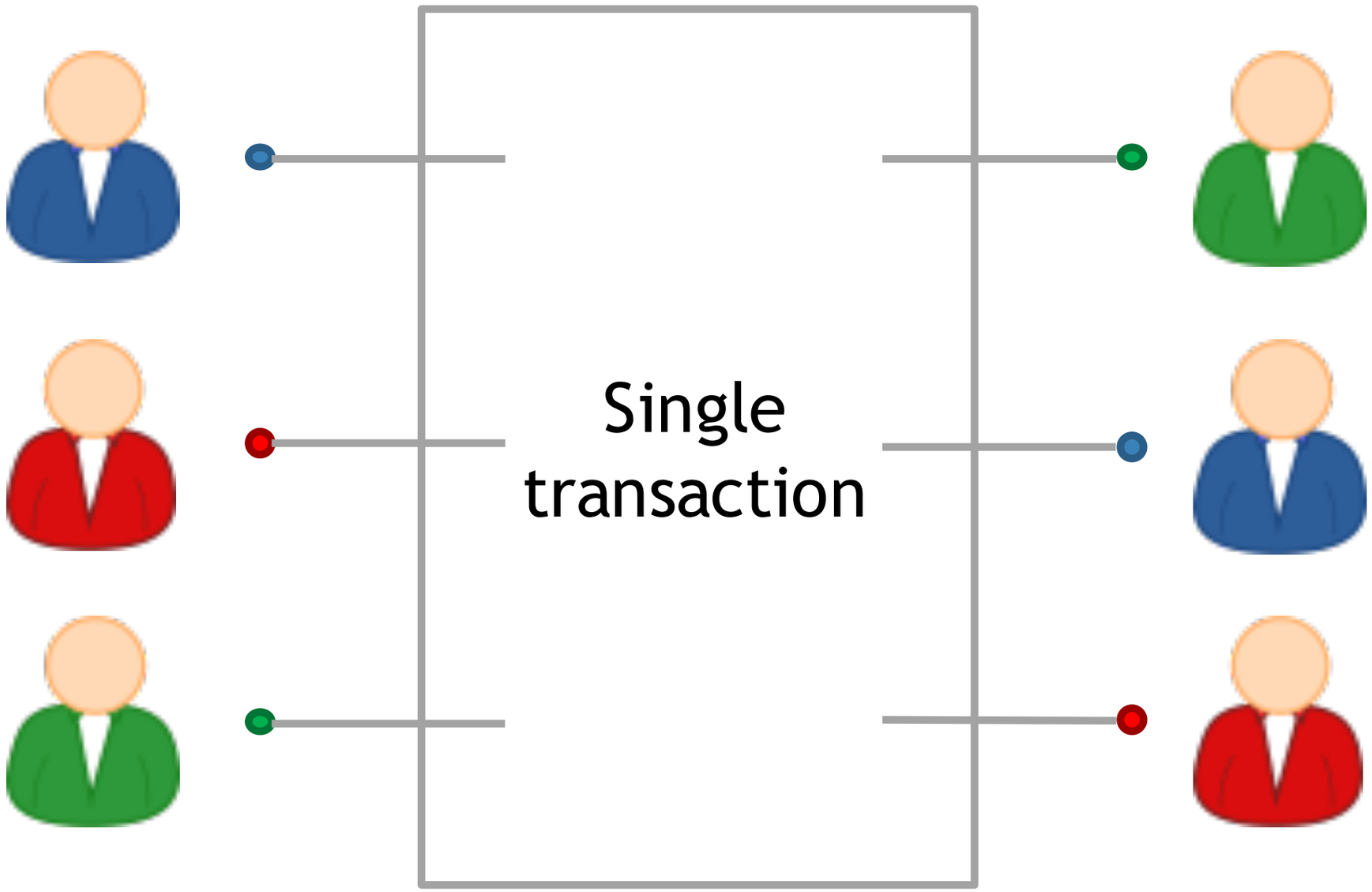
专项服务

多层混币



多重

分布式混币



分布式

提问时间

谢谢！

孙惠平
sunhp@ss.pku.edu.cn