比特币01

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

论文讲解

第三组

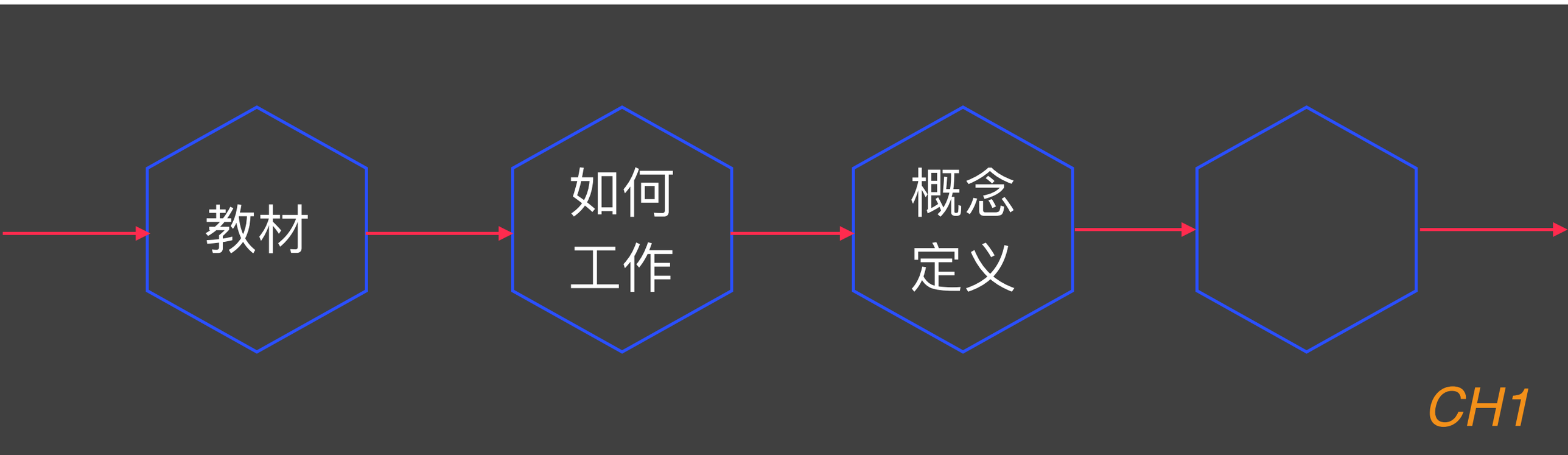
Course Overview

上次课程内容

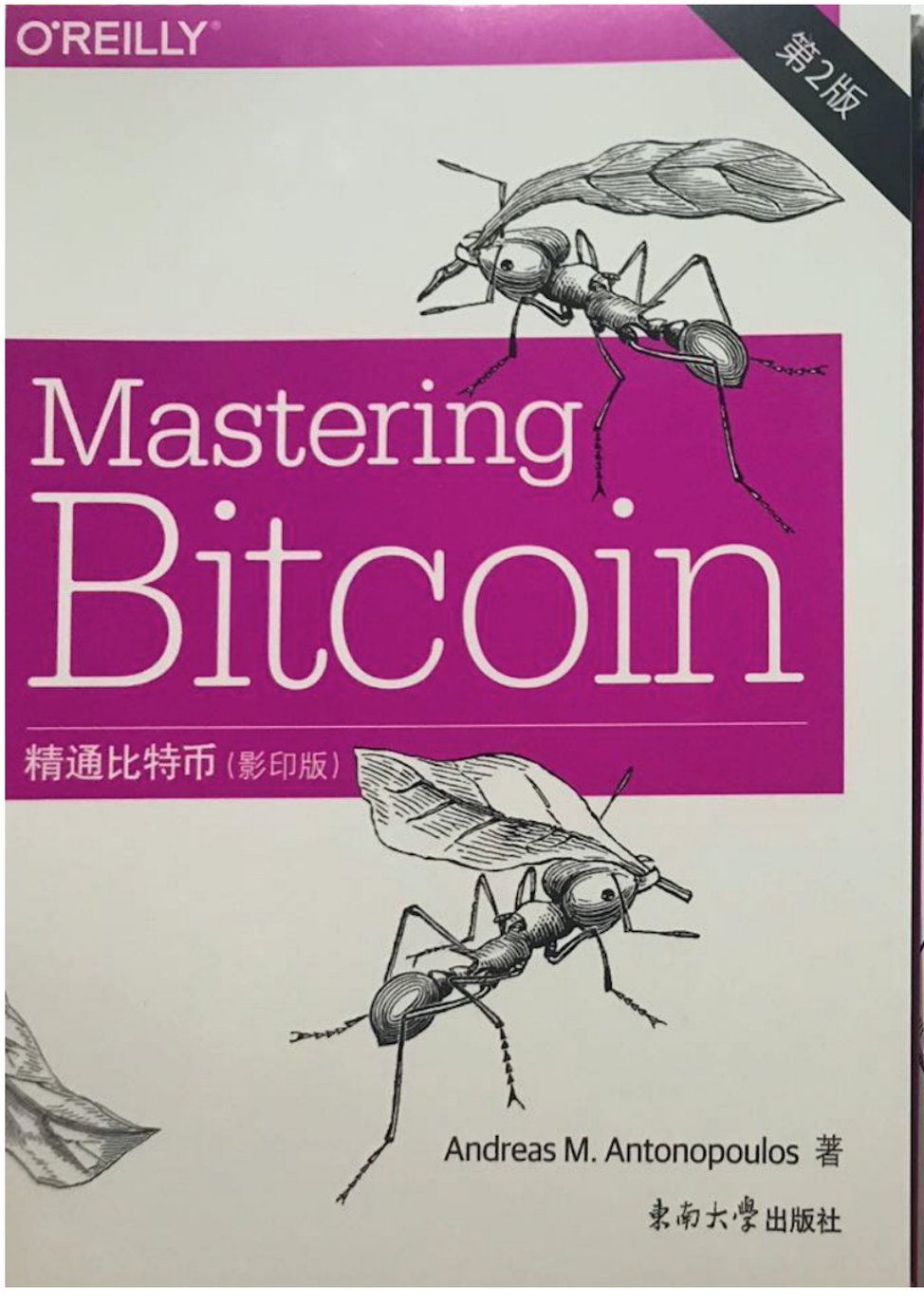
1 史前	2 初识	3 回顾	4 剖析
• 交易 • 交易历史 • 金融创新 • 记账历史	• 区块链定义 • 账本集vs.分 • 区块链结构 • 租车例子	• 区块链起源 • 比特币 • 区块链发展 • 智能合约 • ICO	• 计算视角 • 网络视角 • 是否使用 • 面临挑战

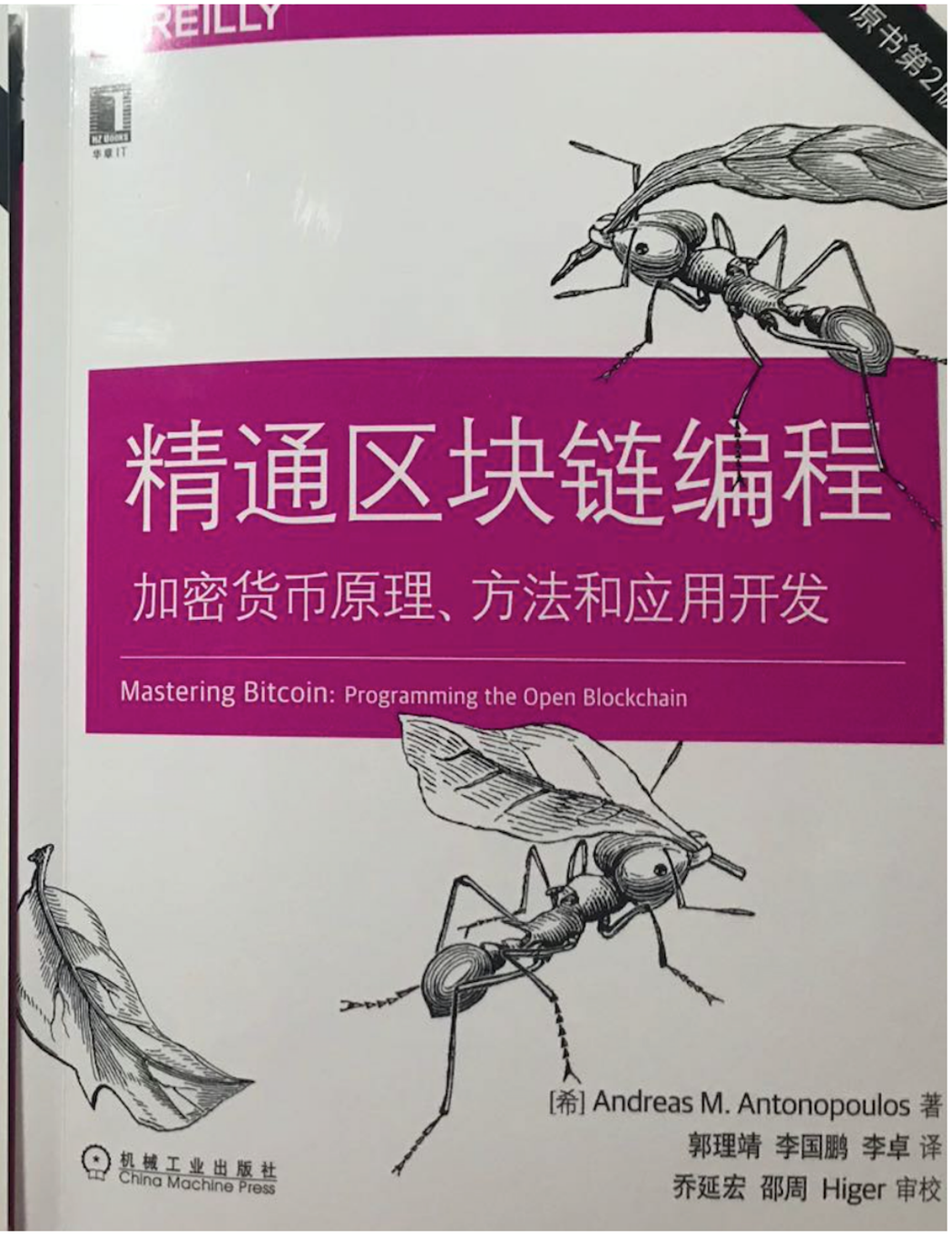
掌握比特币

简介



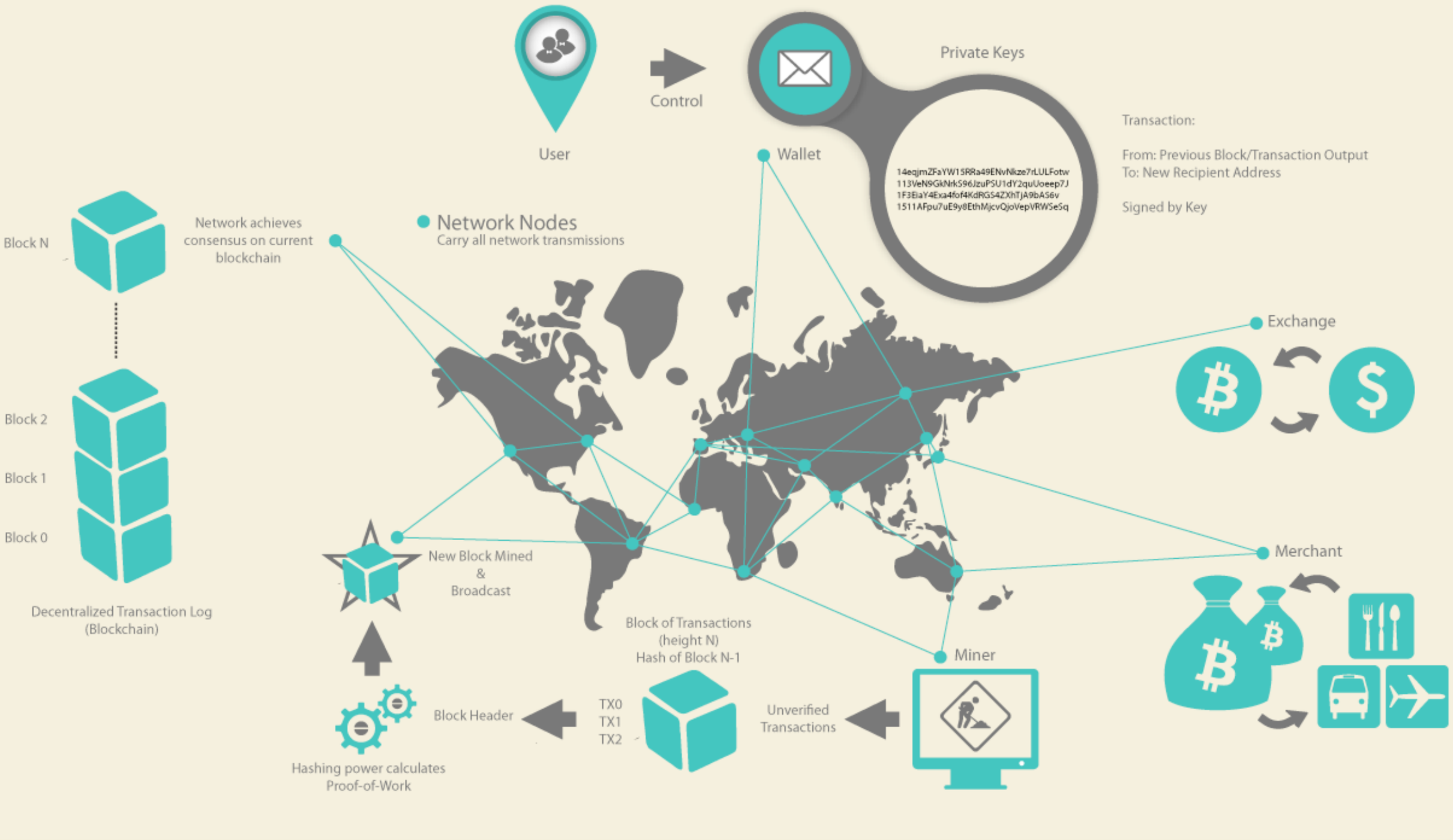
参考书


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



Mastering Bitcoin

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

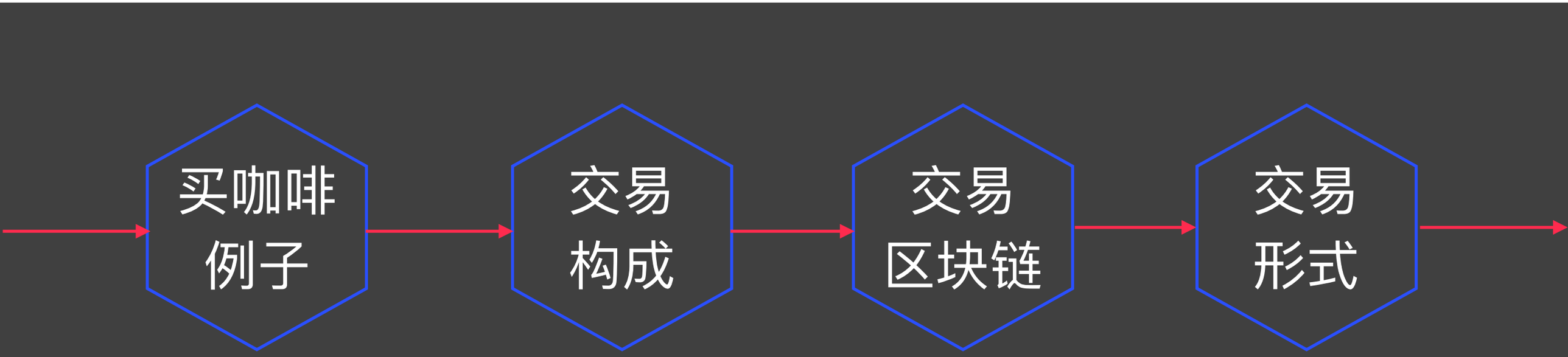
用户通过网络进行比特币进行转账和可以做到和传统货币一样的事情

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

掌握比特币

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

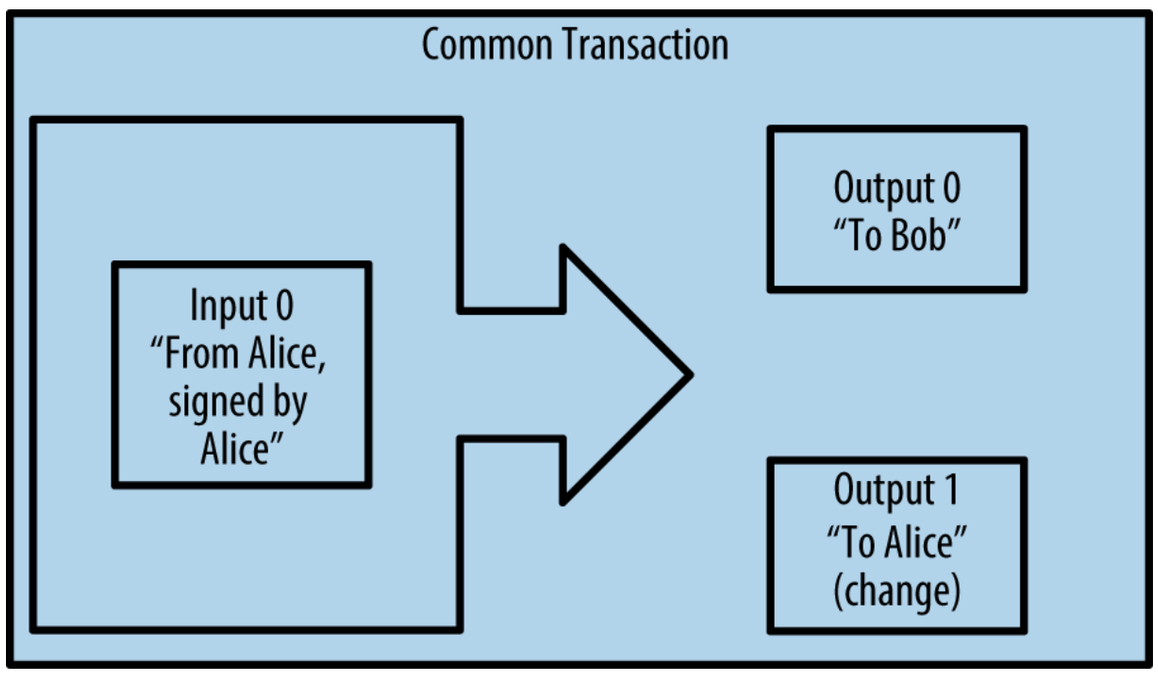
OUTPUTS To

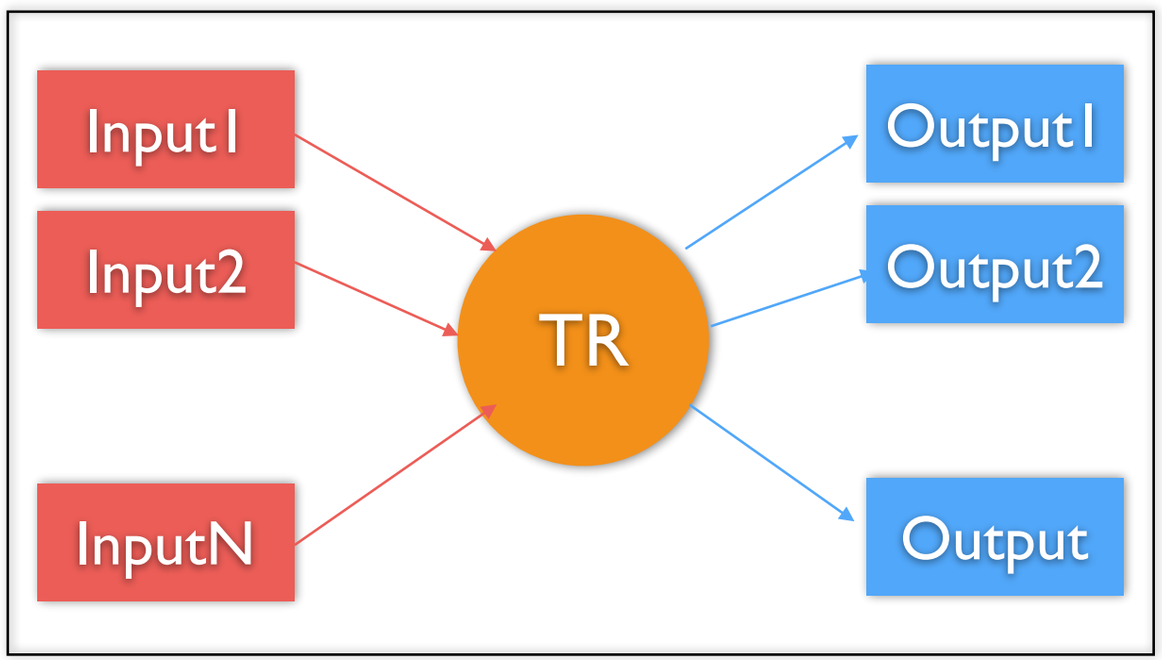
Output #0 Gopesh's Address 0.0100 BTC (unspent)

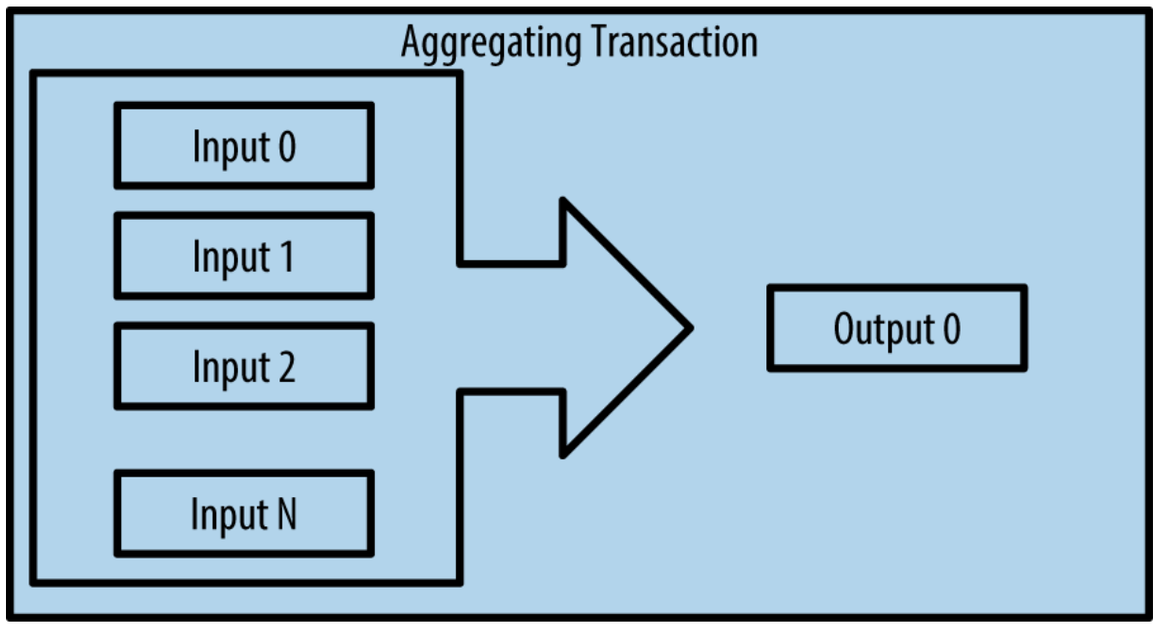
Output #1 Bob's Address (change) 0.0045 BTC (unspent)

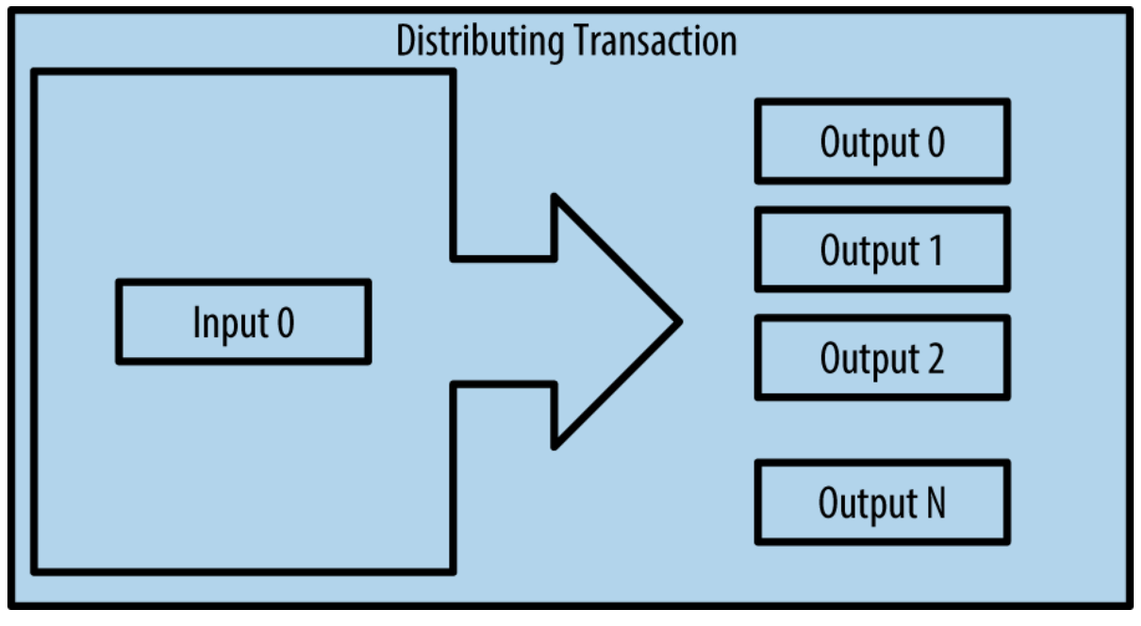
Transaction Fees: 0.0005 BTC

交易形式


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


Input1
Input2
InputN
TR
Output1
Output2
Output


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


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

交易描述

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

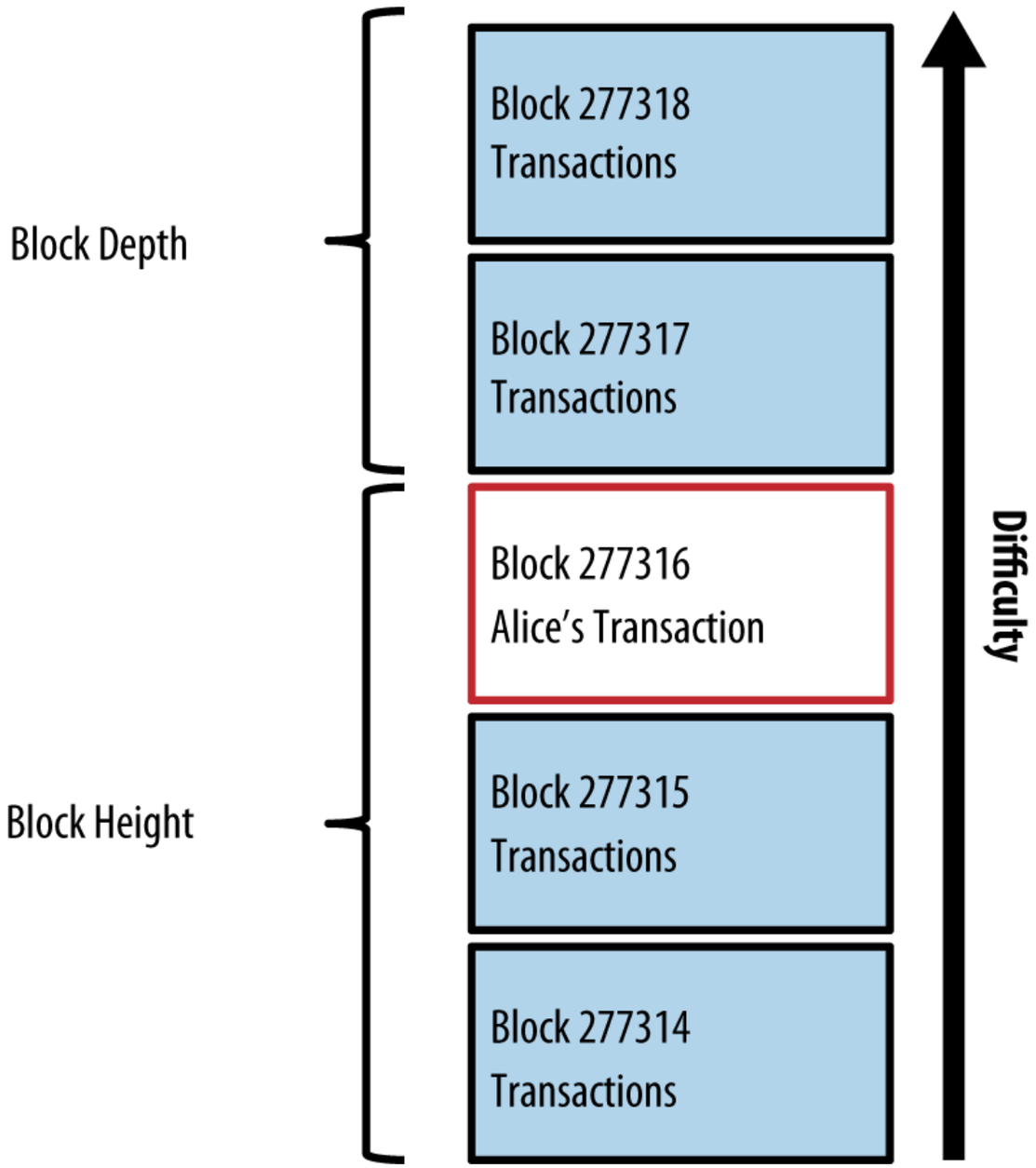
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

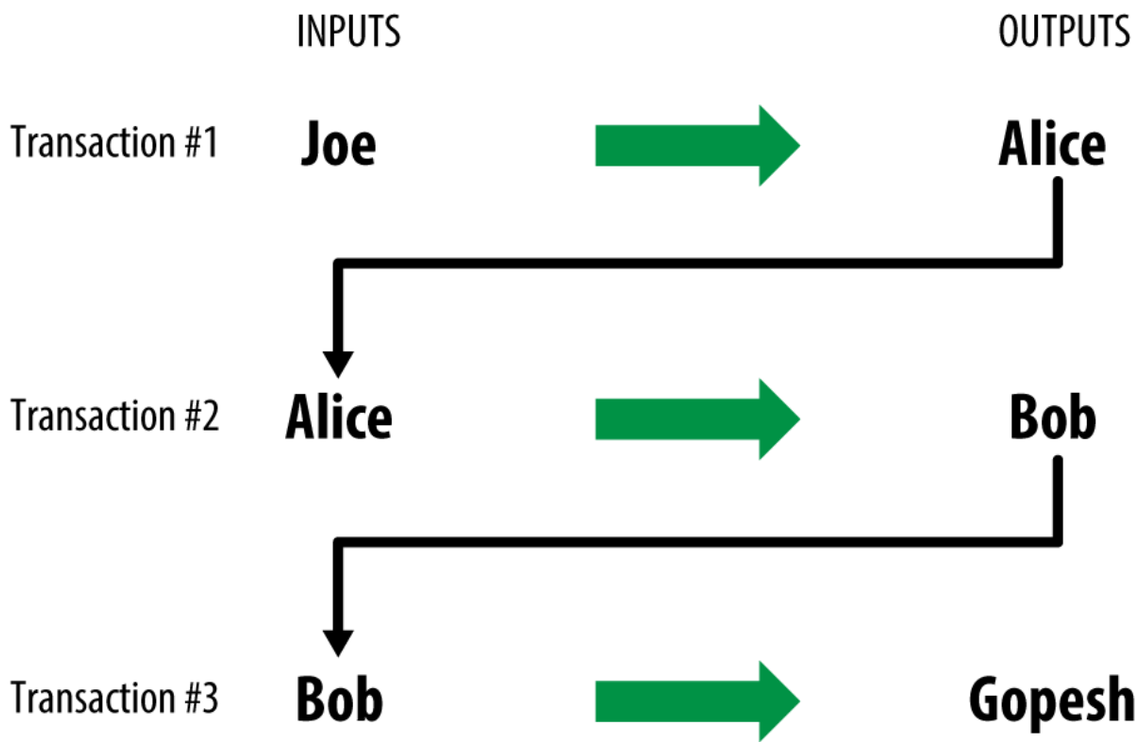
97 Confirmations | 0.0995 BTC

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

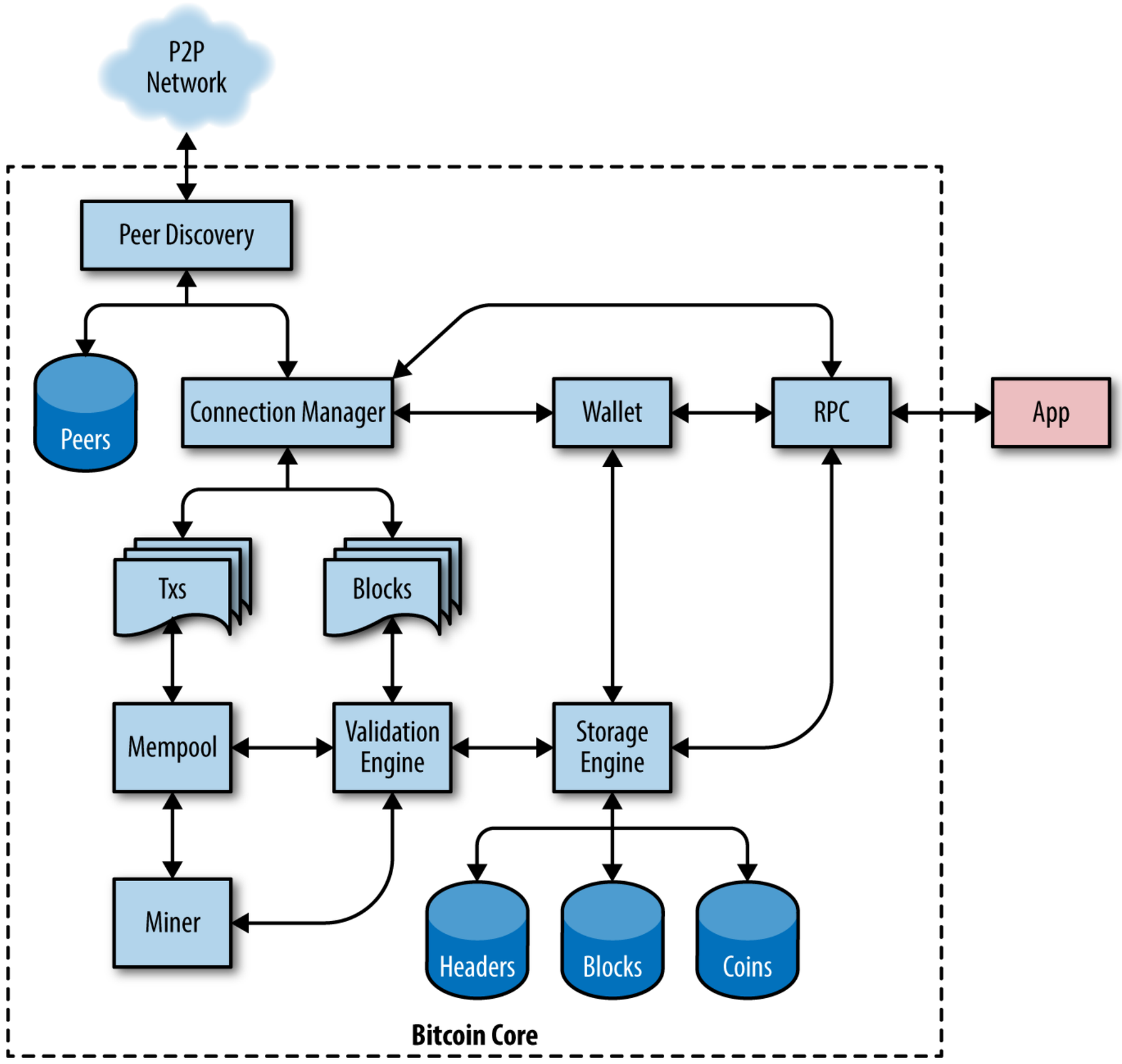
区块和链条


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

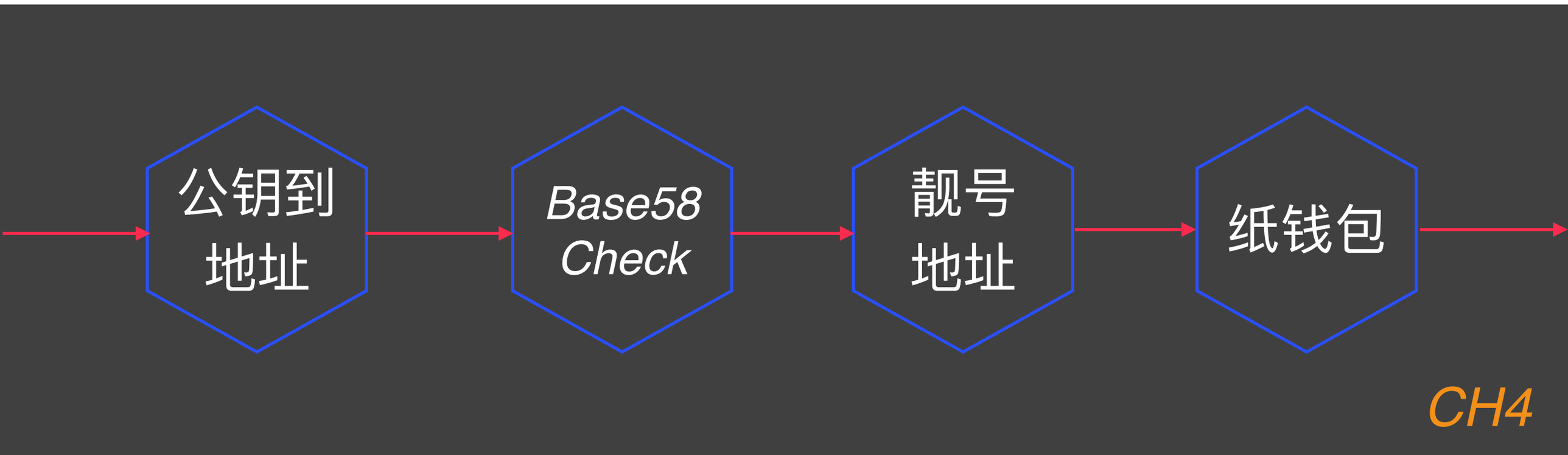

INPUTS
OUTPUTS
Transaction #1
Joe
Alice
Transaction #2
Alice
Bob
Transaction #3
Bob
Gopesh

掌握比特币核心客户端

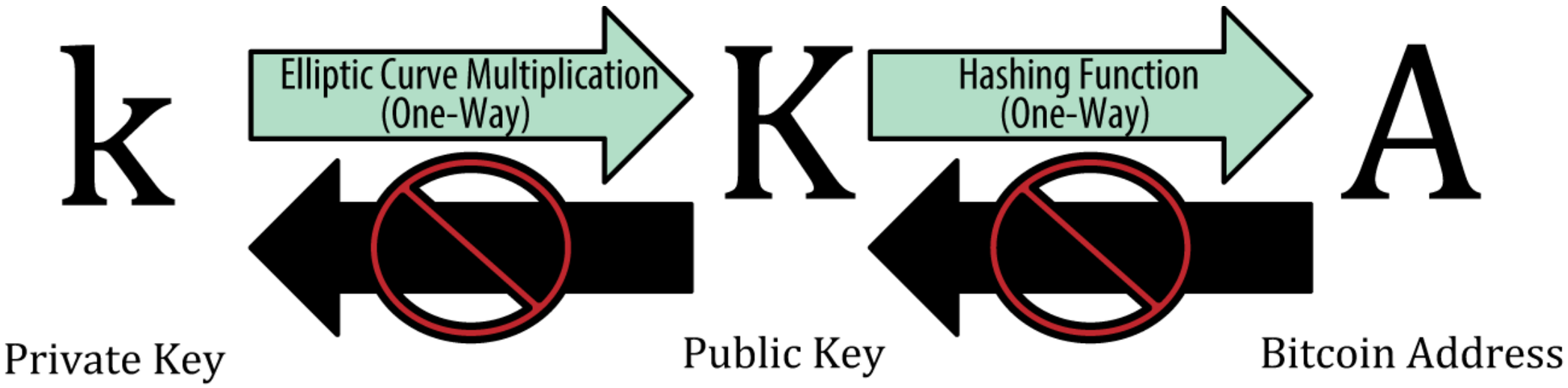
Bitcoin核心架构



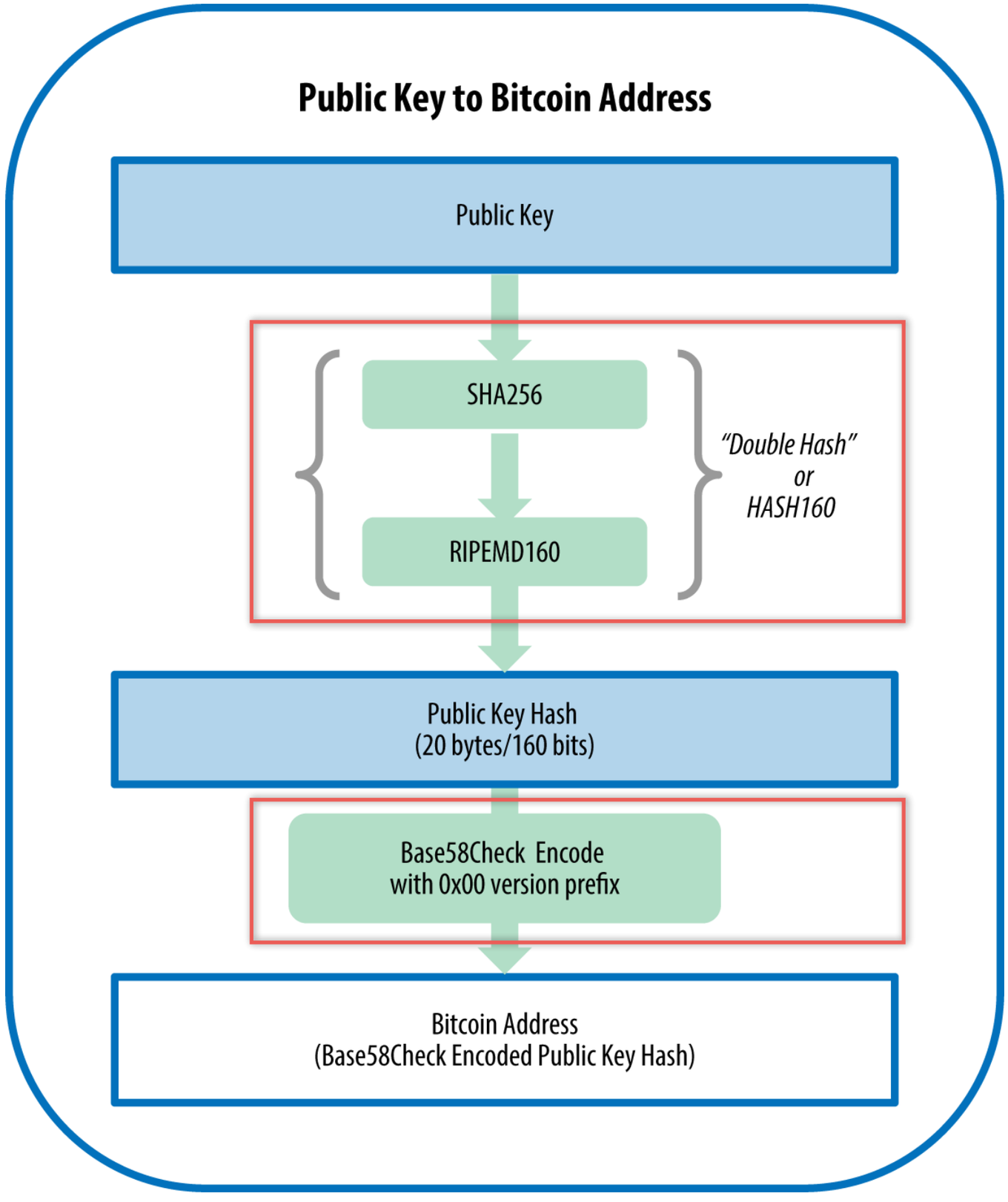
掌握比特币密钥和地址



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

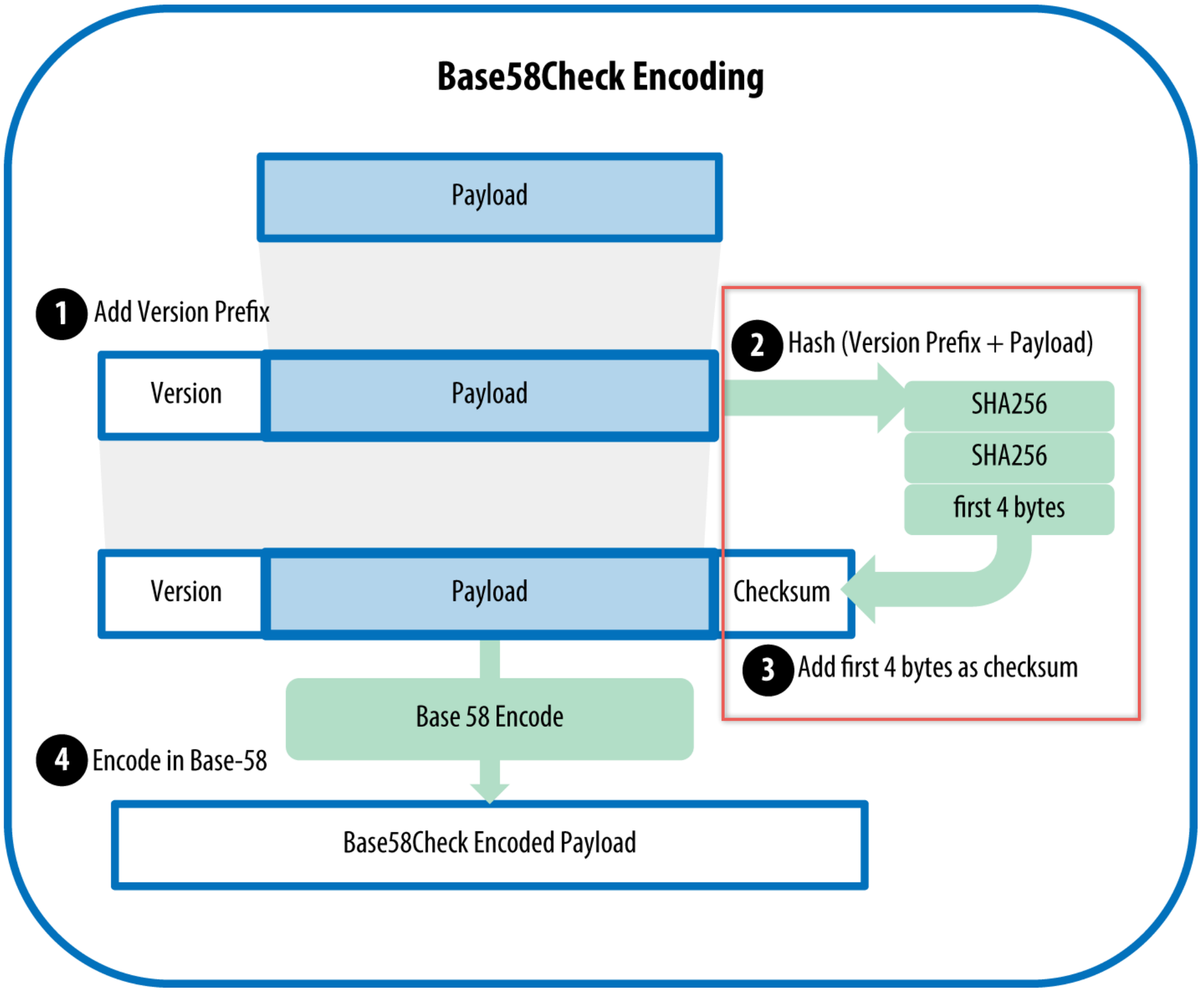
- 大写字母
- 小写字母
- 数字
- +、/

Base58

- 0和o
- I和l

Base58Check

- 检验和

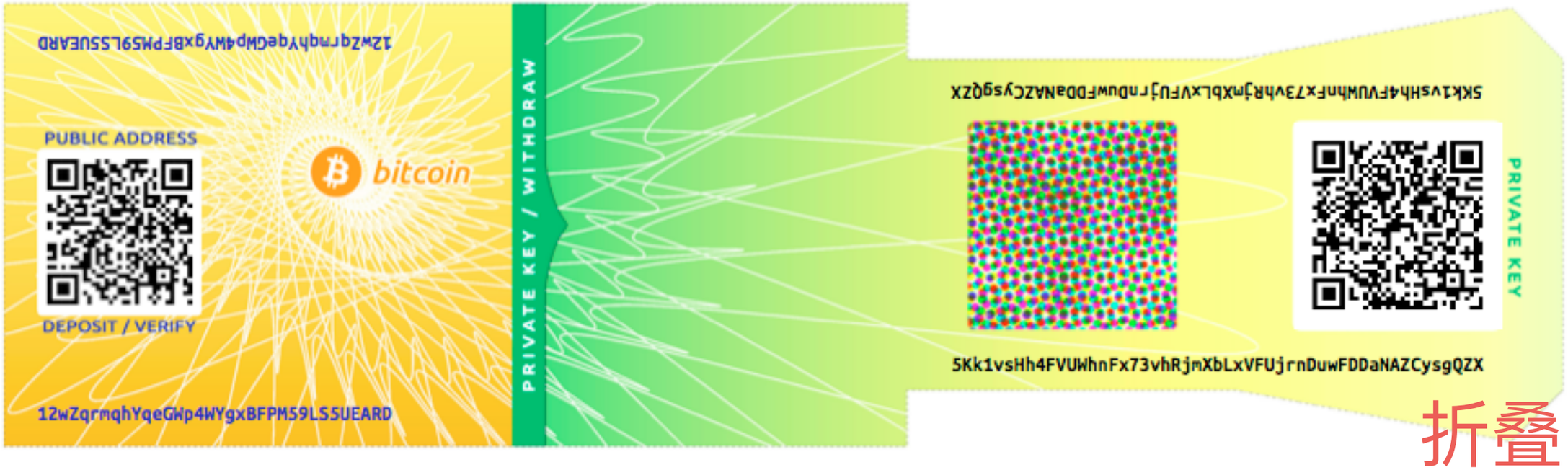


靓号地址

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



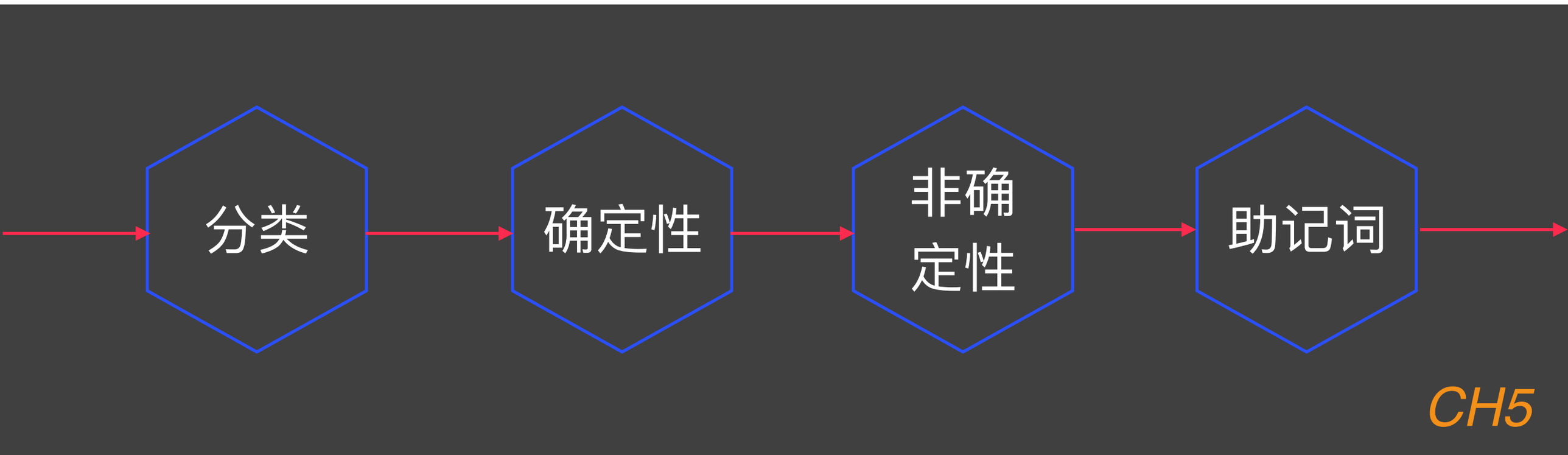
折叠

纸钱包

私钥
密封

多个副本

钱包



钱包

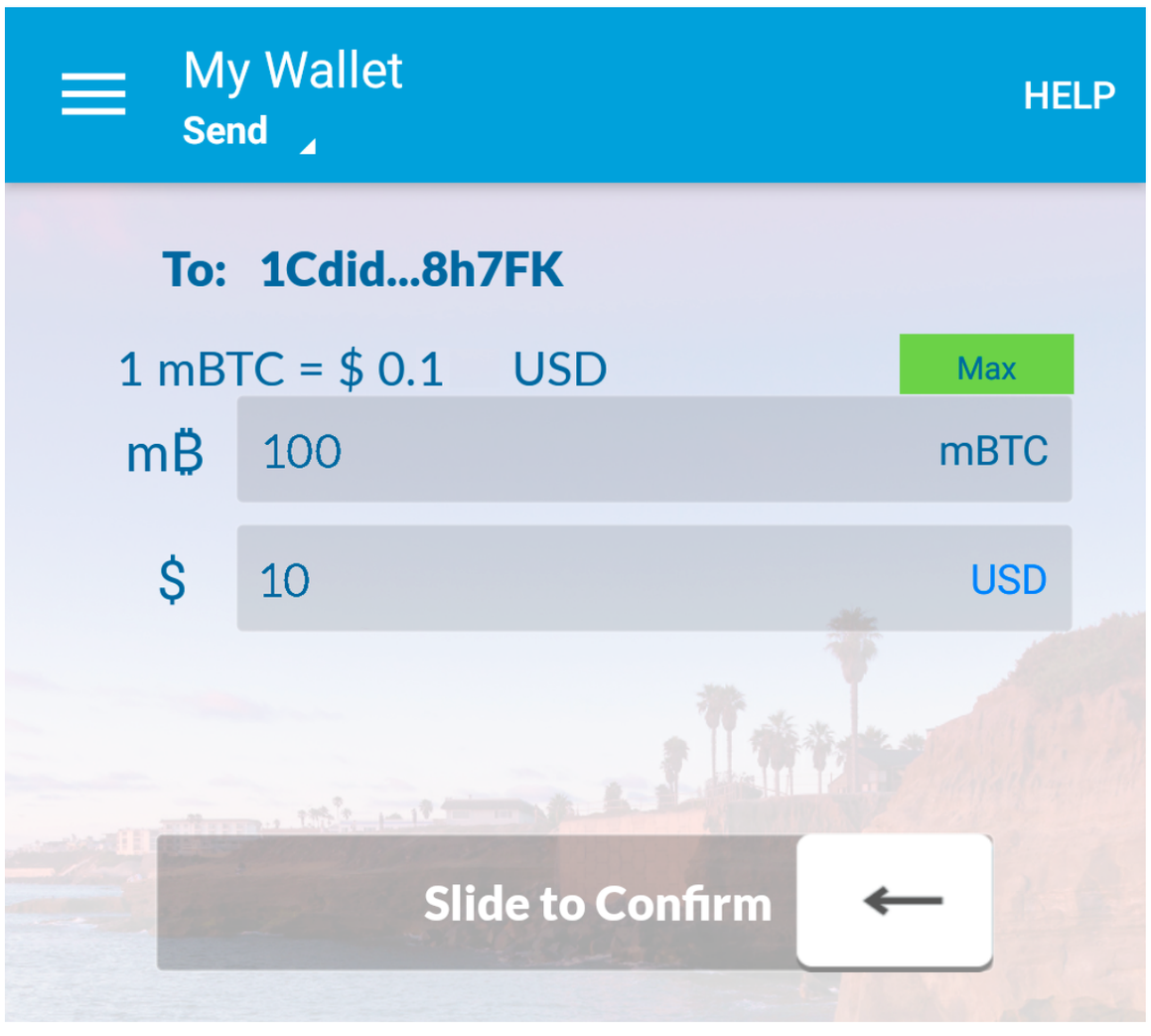
桌面钱包

手机钱包

网络钱包

硬件钱包

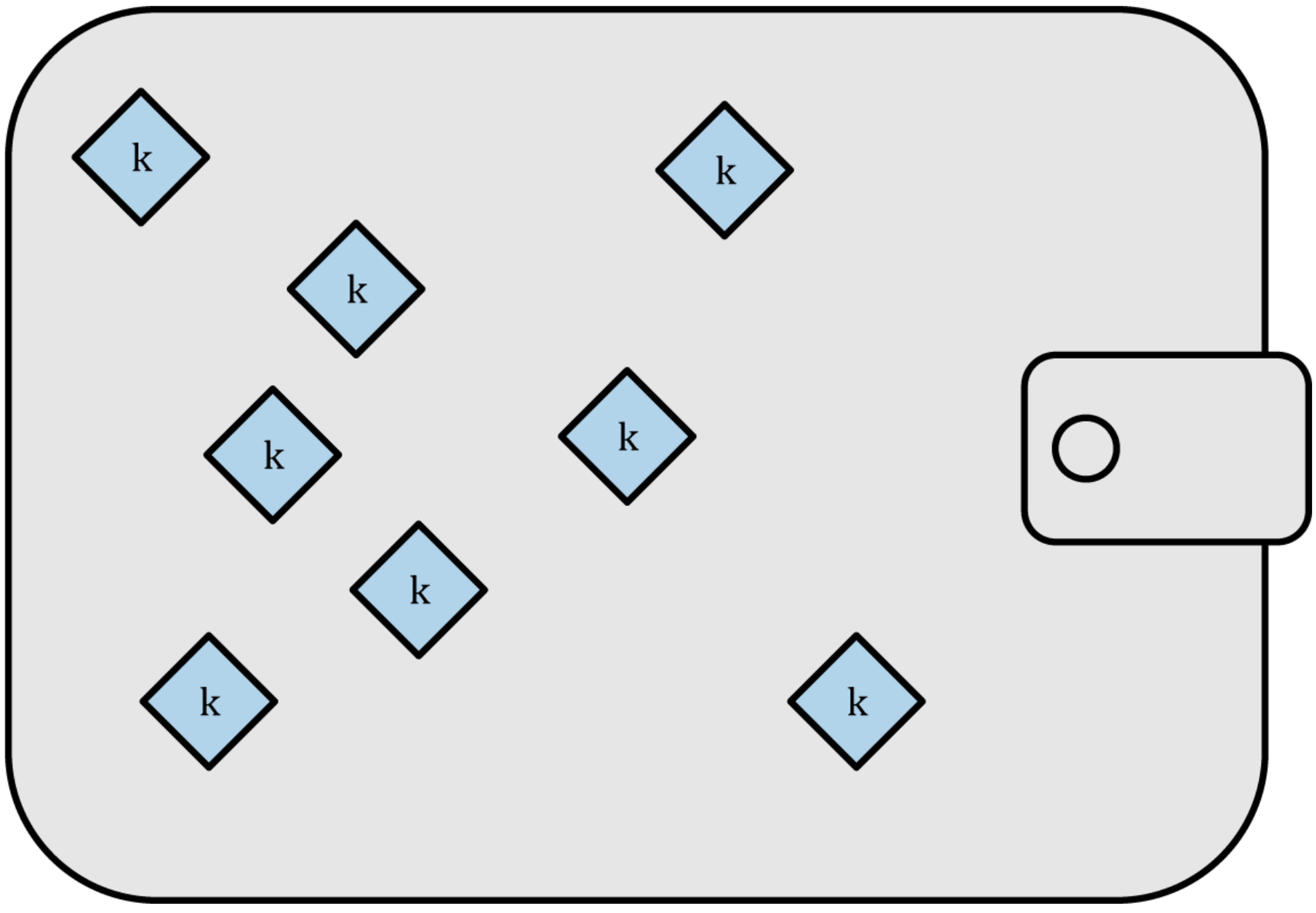
纸钱包



非确定性钱包

随机钱包

JBOK
Just a Bunch of Keys

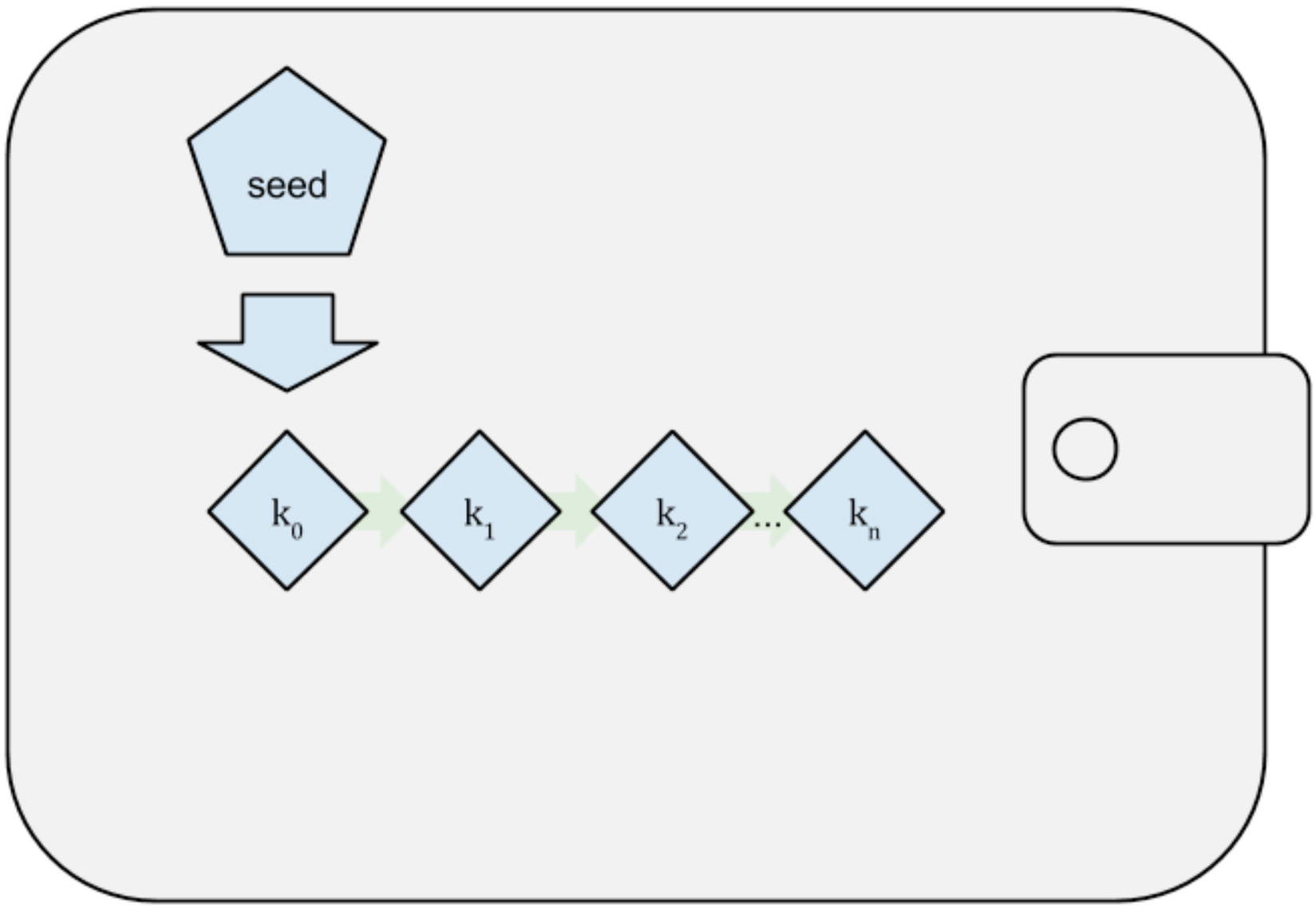


难于管理、备份和导入

确定性钱包

种子钱包

种子
—串随机生
成的数字

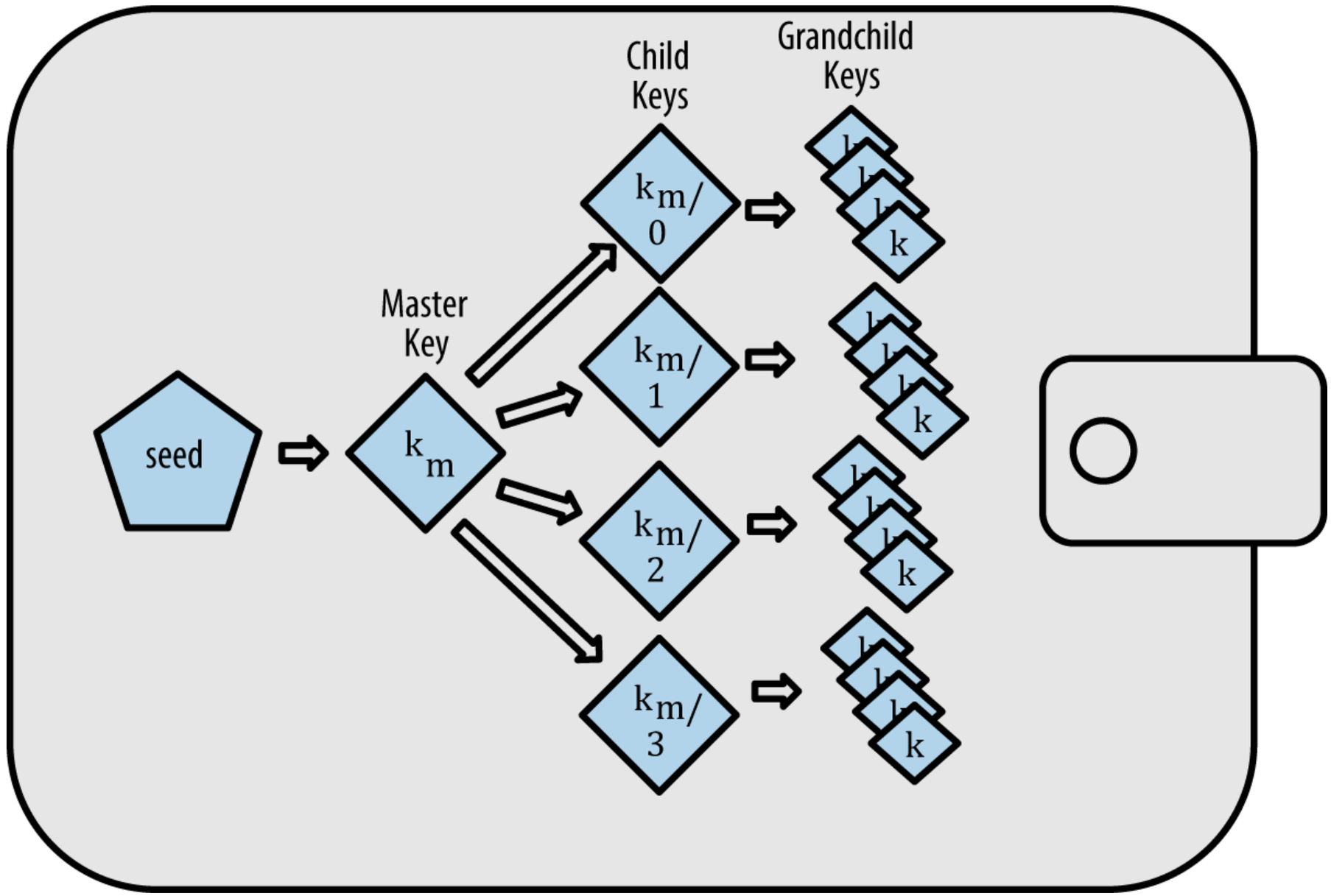


分层确定性钱包

HD钱包

BIP-32
BIP-43
BIP-44

BIP-39

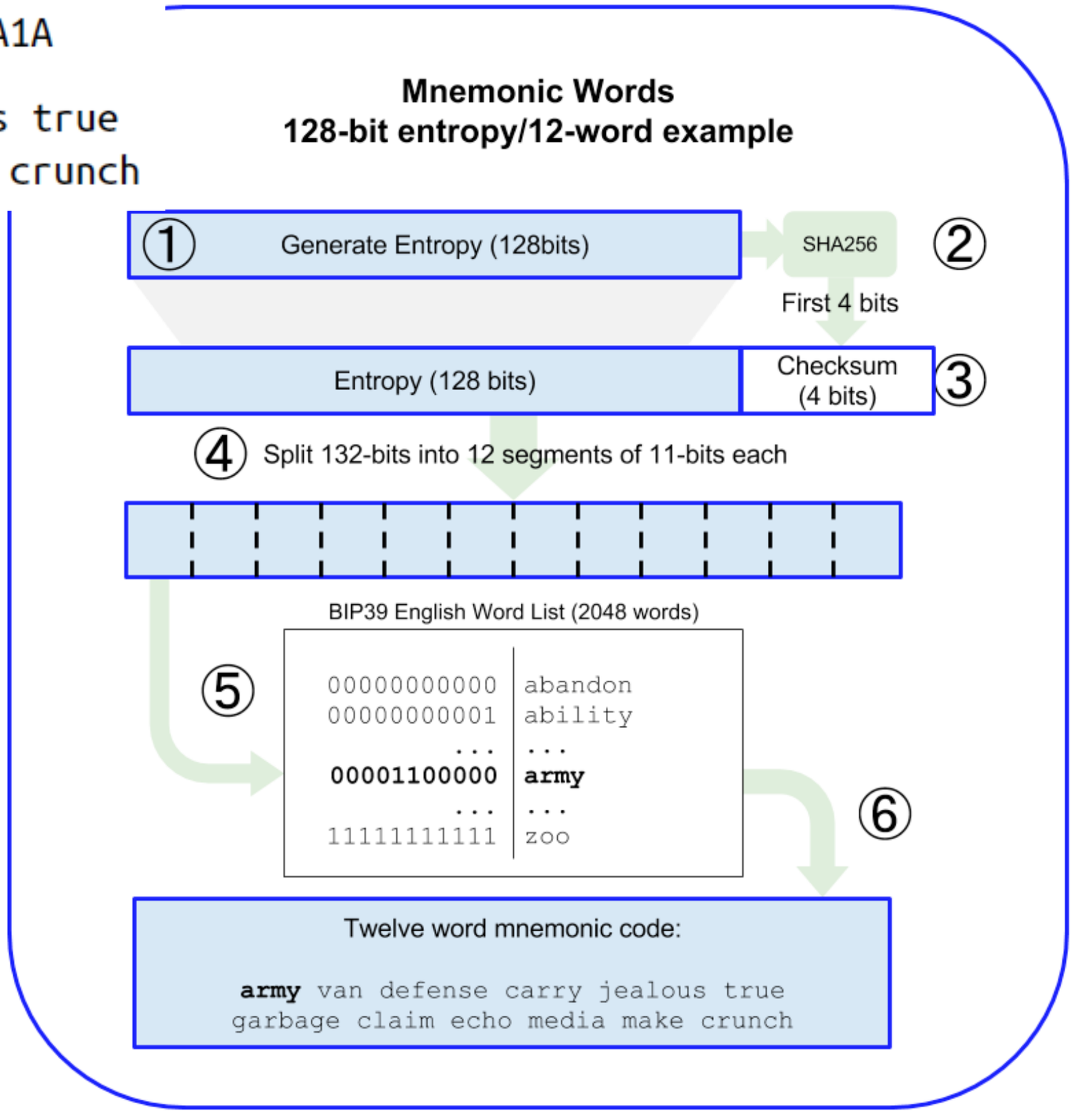


助记词

```
0C1E24E5917779D297E14D45F14E1A1A

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

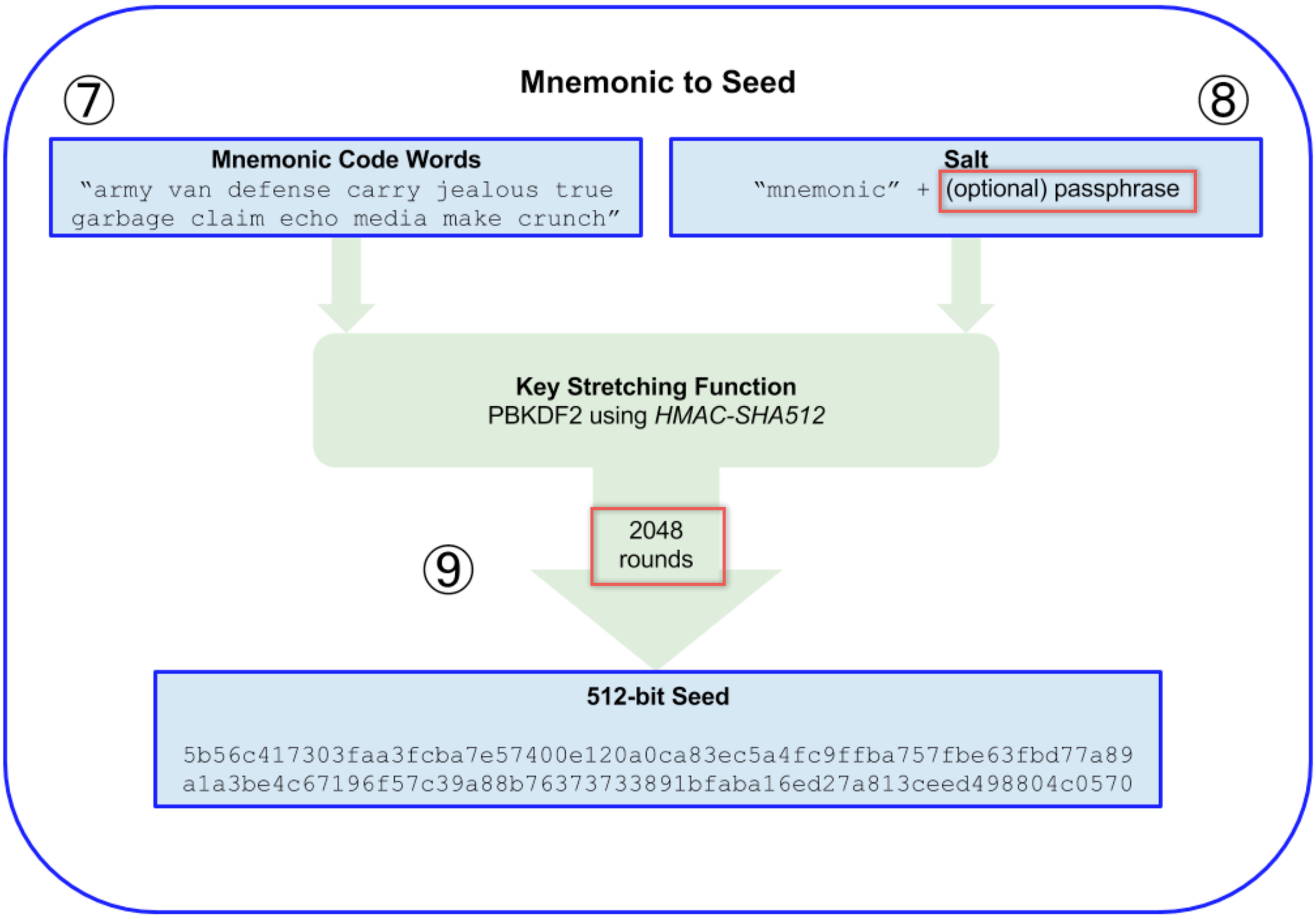
1. *army*
2. *van*
3. *defense*
4. *carry*
5. *jealous*
6. *true*
7. *garbage*
8. *claim*
9. *echo*
10. *media*
11. *make*
12. *crunch*



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

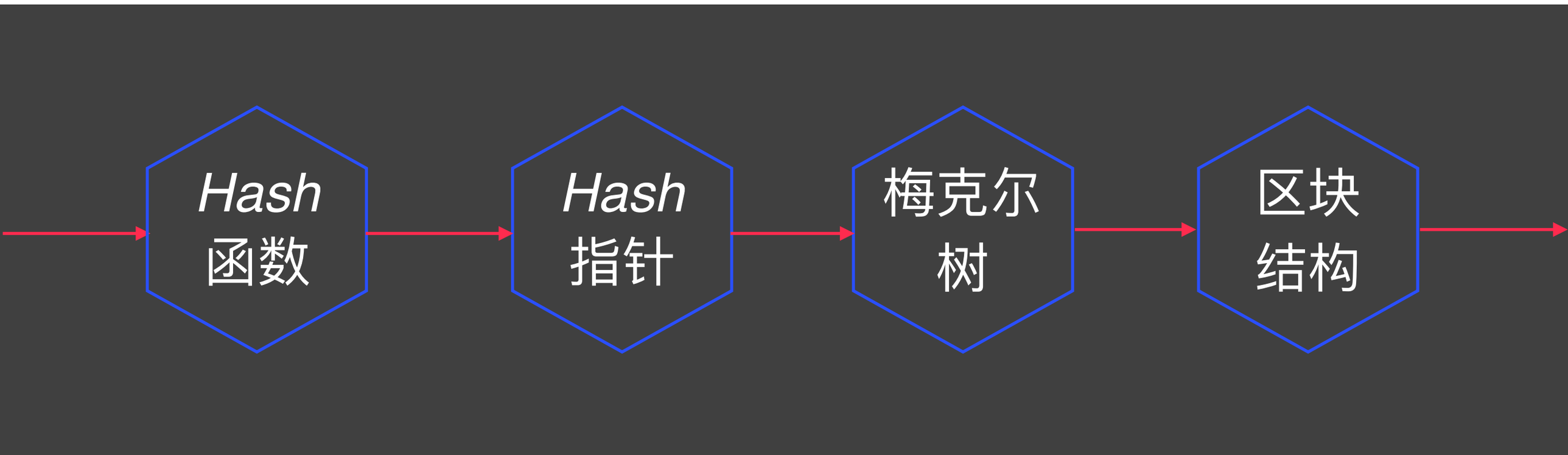
Bitcoin

BIP32 Root Key

xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6
i6ddYjb5PLtUdMZn8LhvuCVhGcQntq5rn7JVMqnie

https://iancoleman.io/bip39/

区块

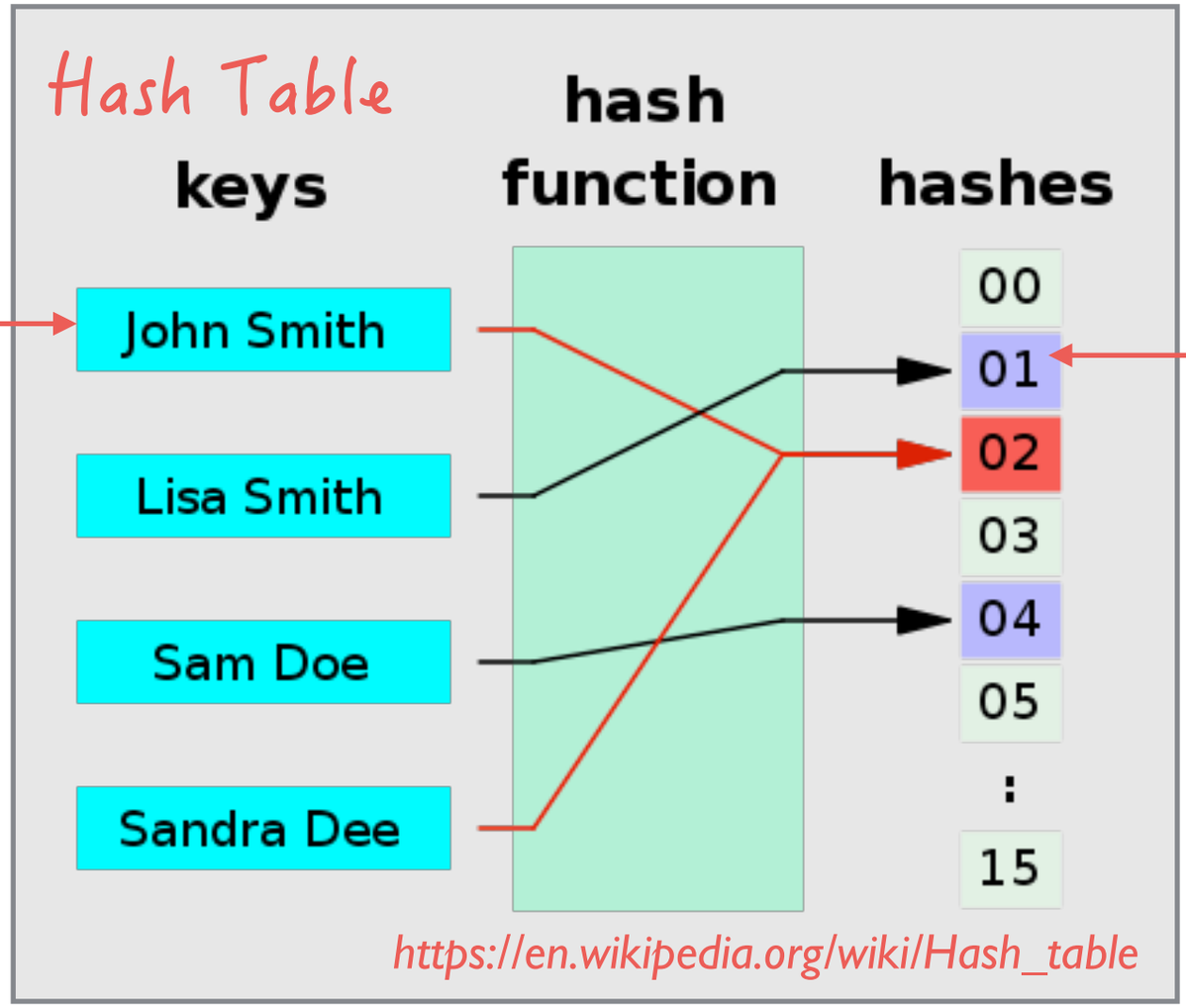


Hash函数

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

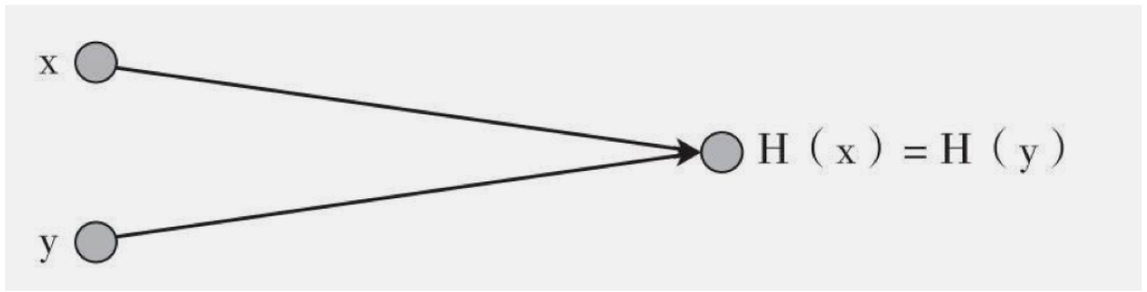
MEM2018 → SHA256 → 547d71f91fec62c23dee84cf2a5dcfd4bdc46a05b2ddd3253555c1b76be433e5

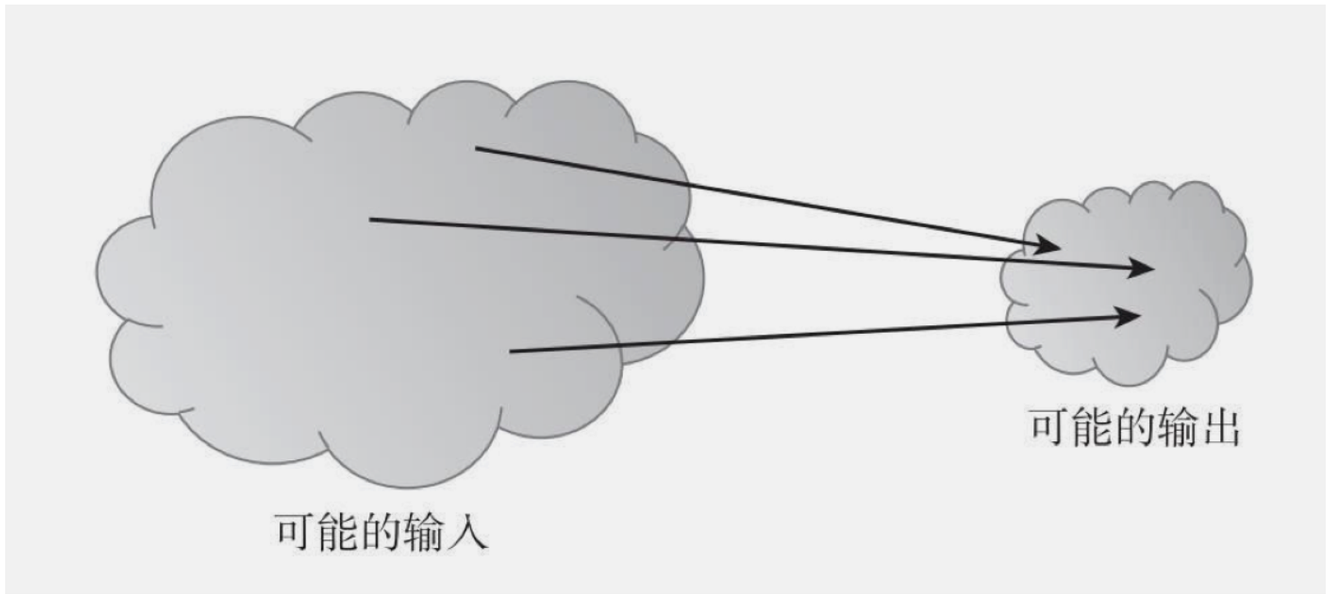
单向性

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

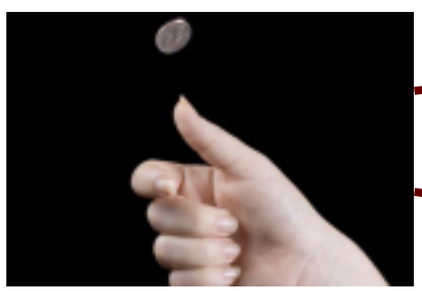
Hash函数

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

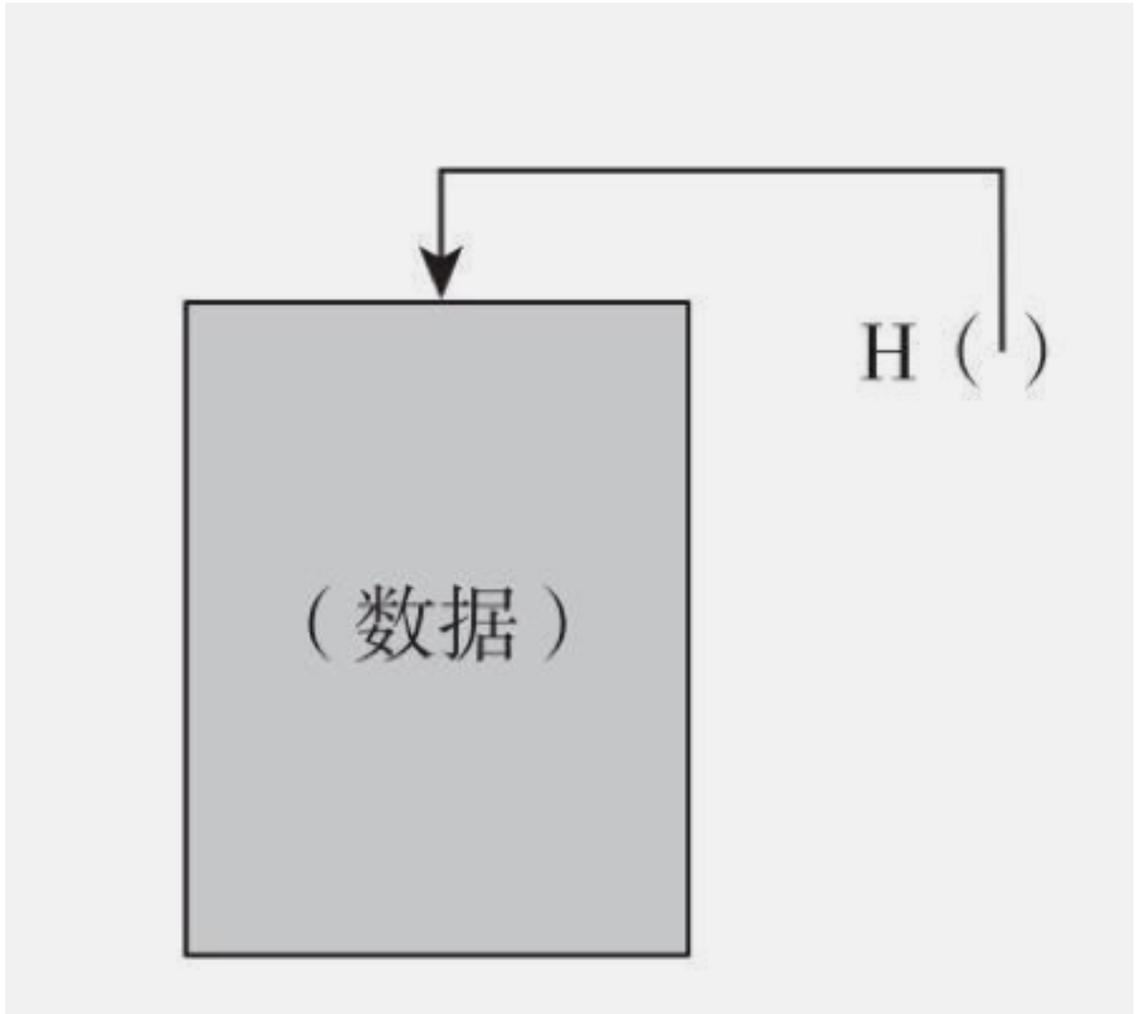
难题友好

Hash指针

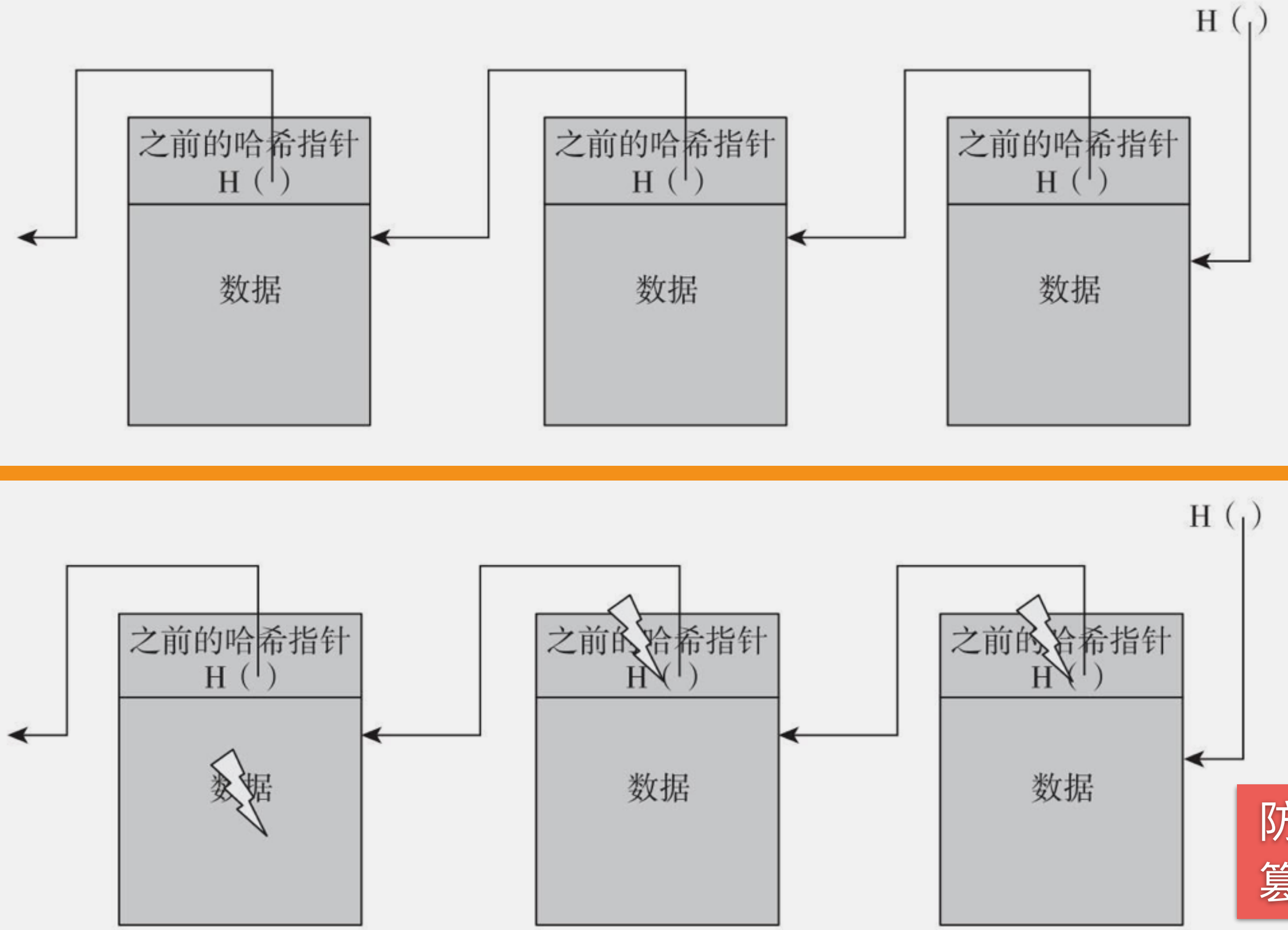
Hash指针：
是一个指向存储数据
及其数据Hash的指针

取回数据
验证数据是否改变

区块链的关键思想

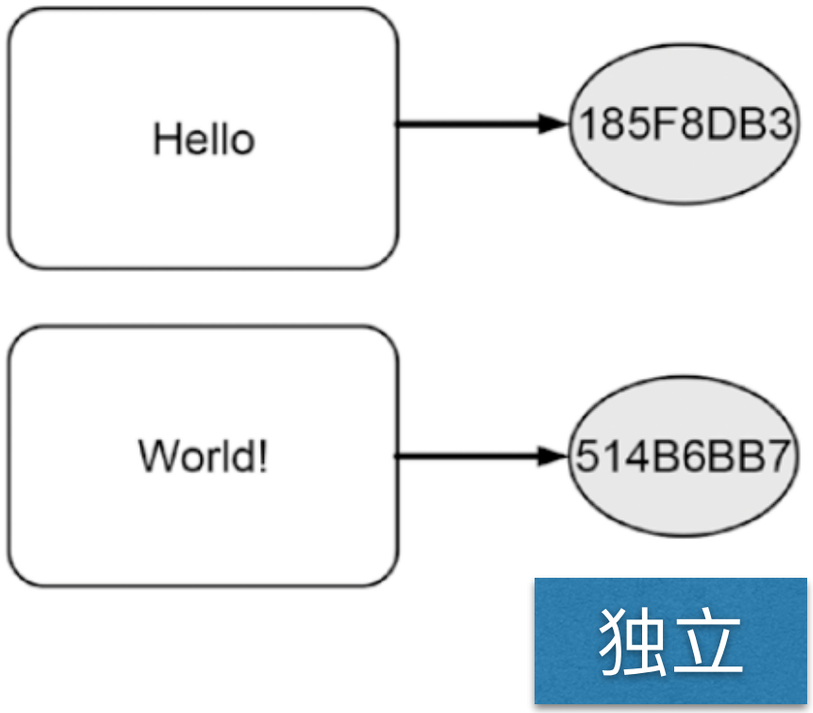


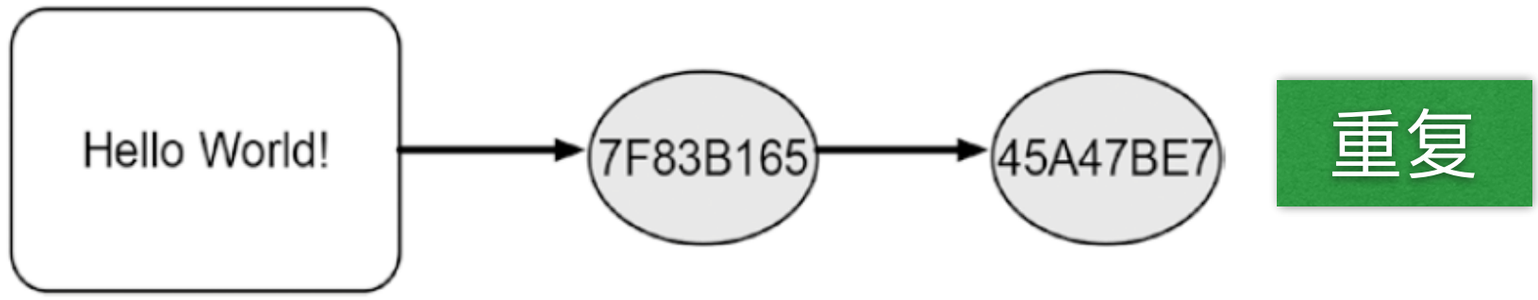
区块链

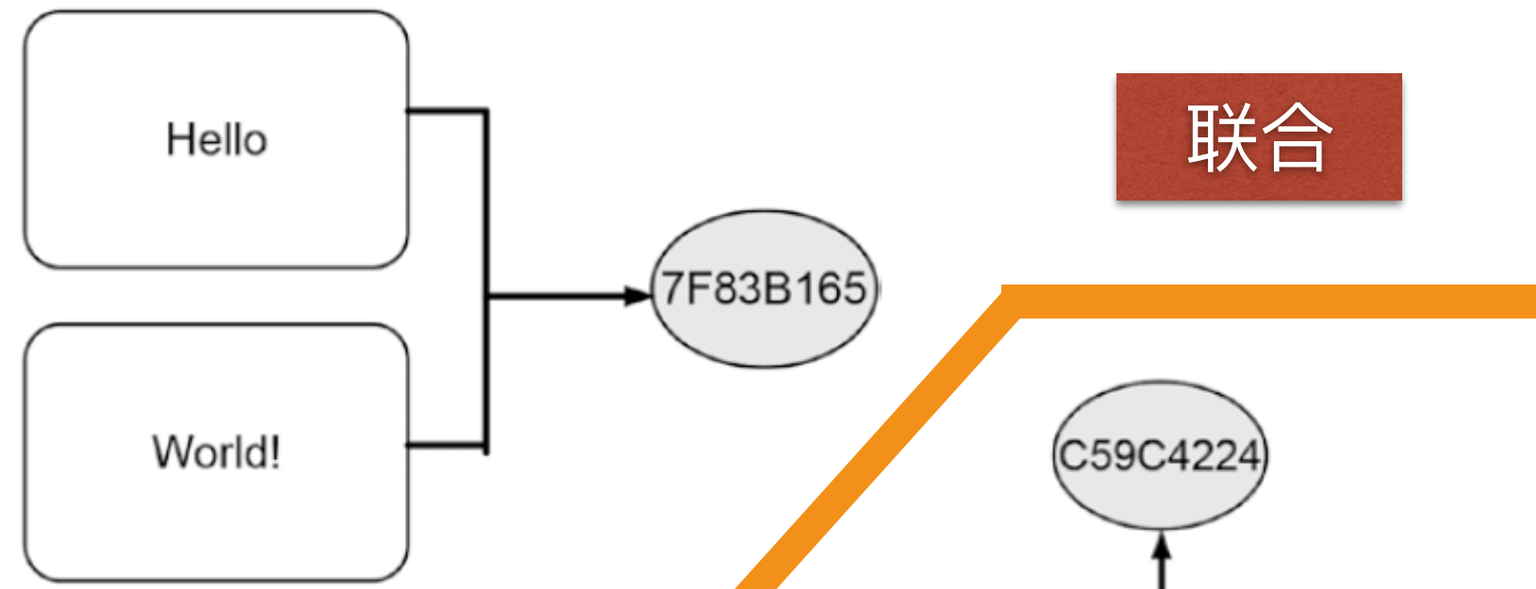

H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
H（）
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
之前的哈希指针
H（）
数据
防止
篡改

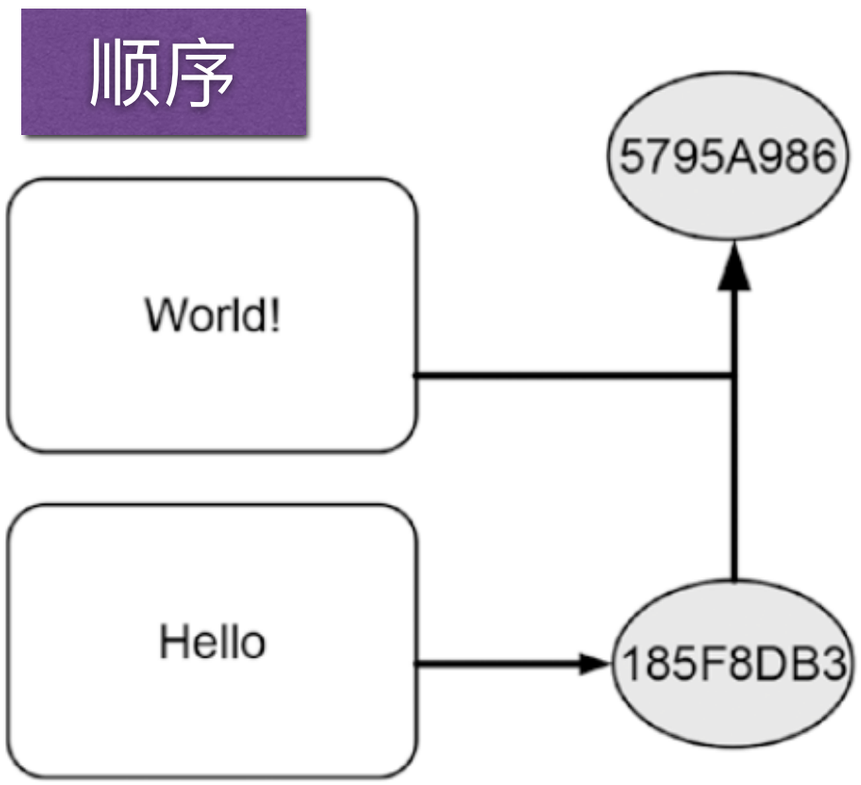
Hash数据模式

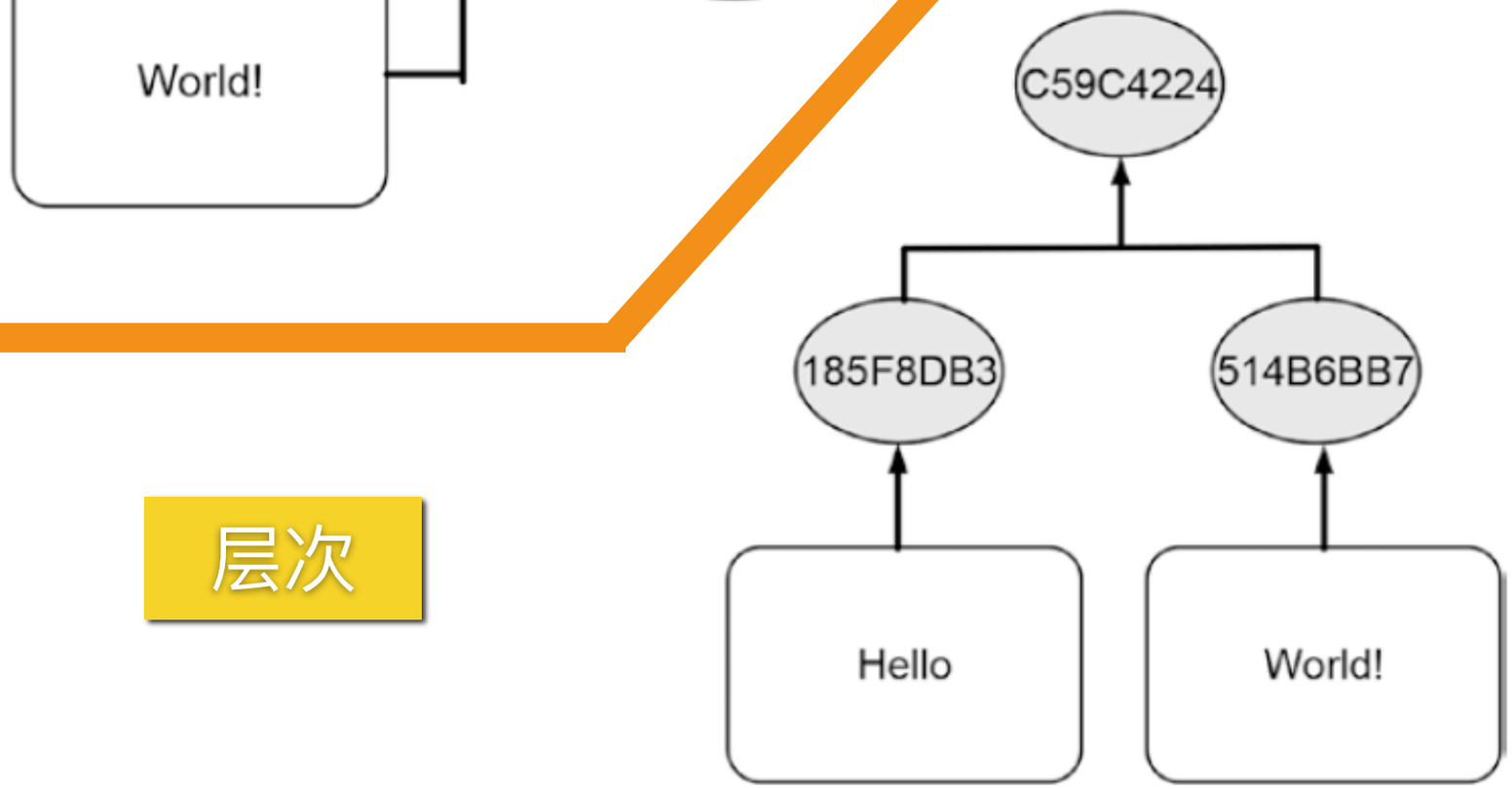
Blockchain Basics:A Non-Technical Introduction in 25 Steps @ APRESS



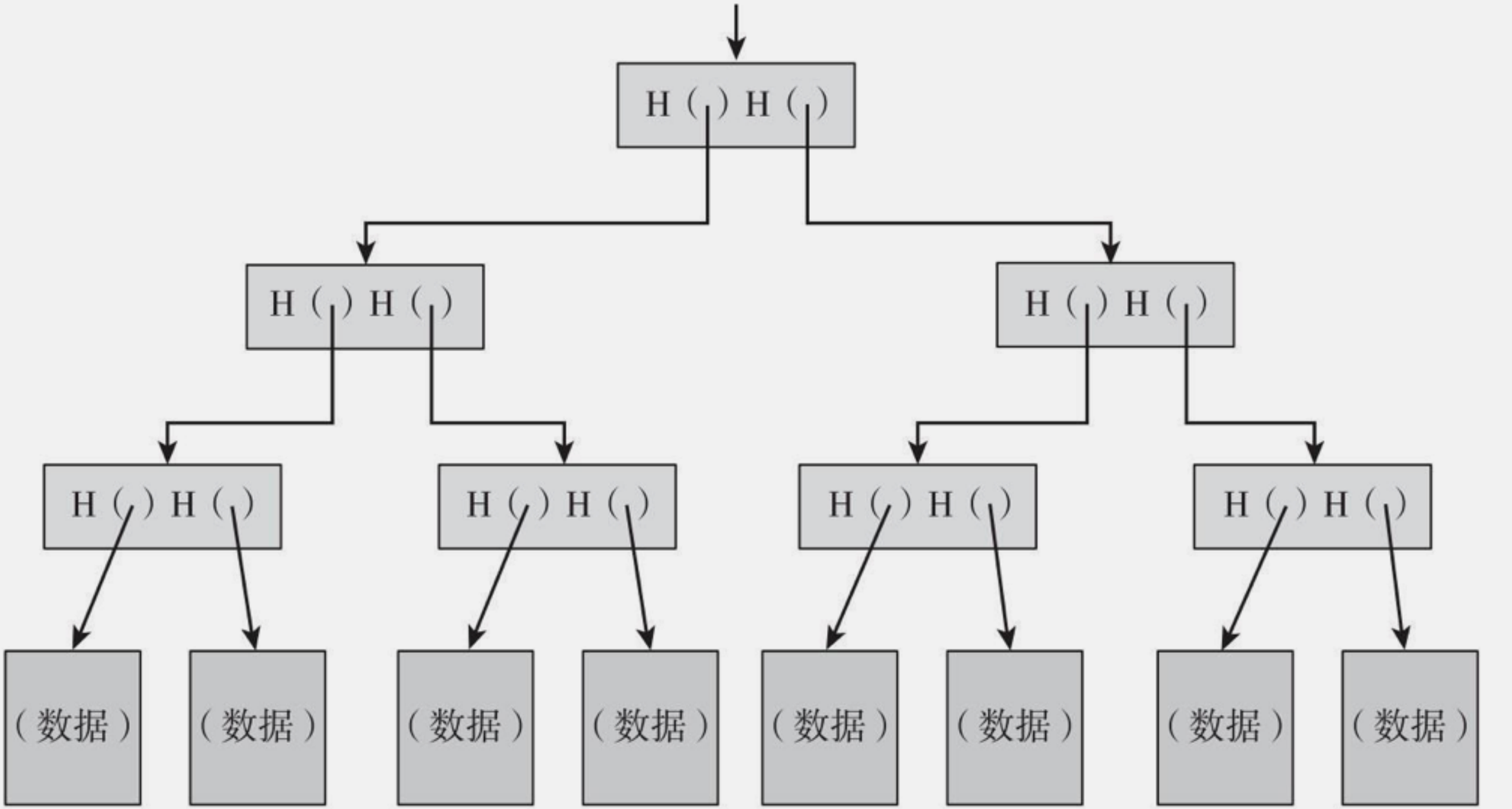




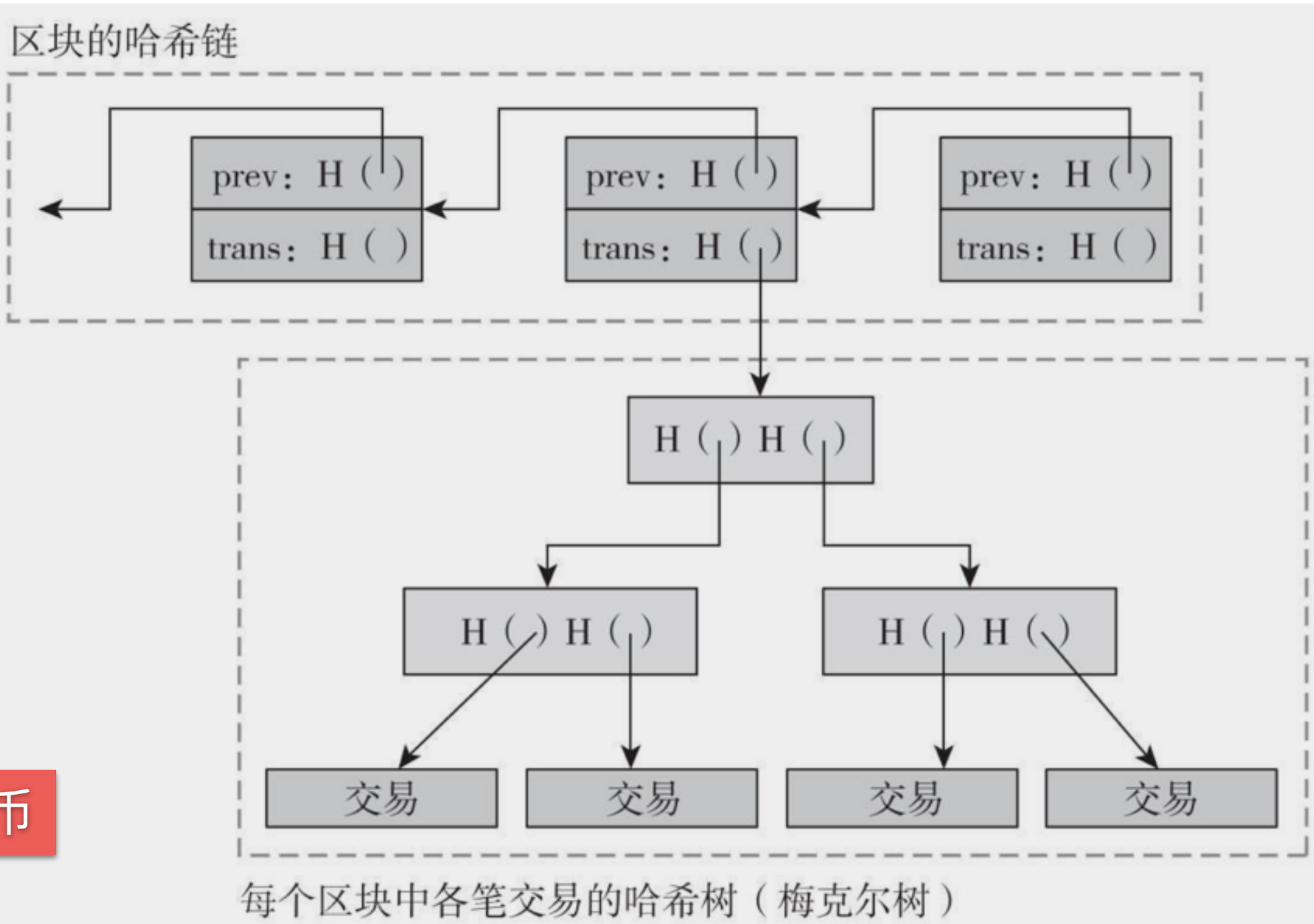




梅克尔树



区块结构

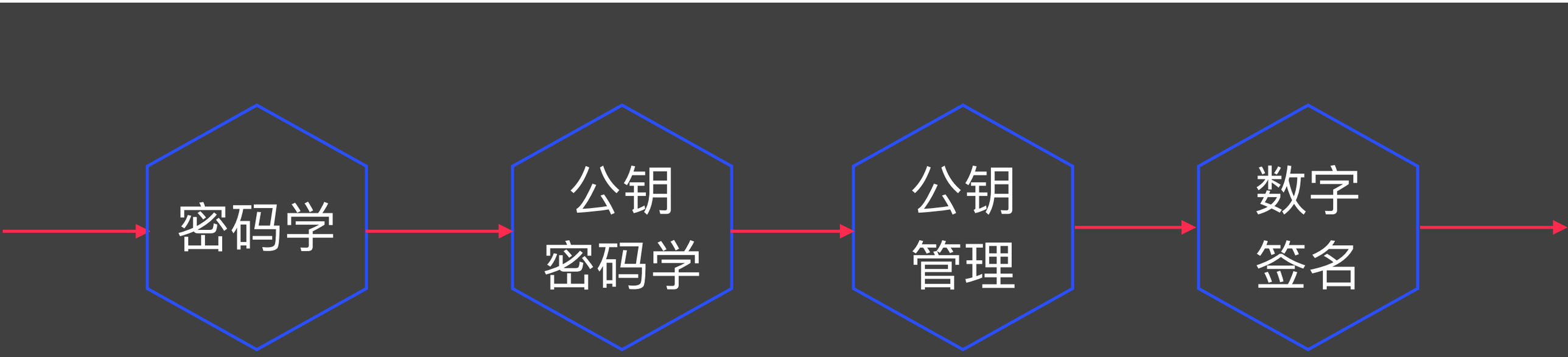


比特币

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。

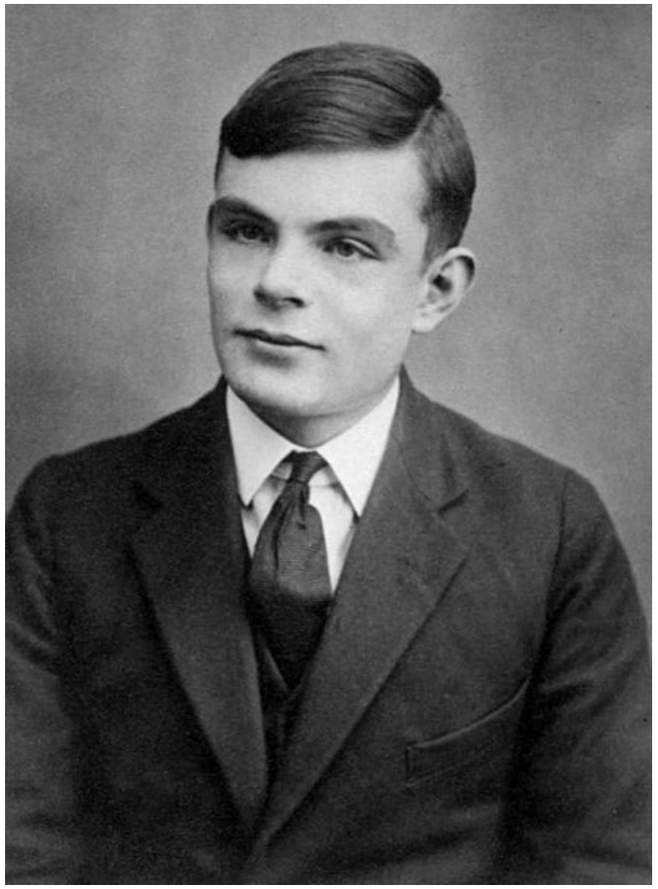
密码



密码学

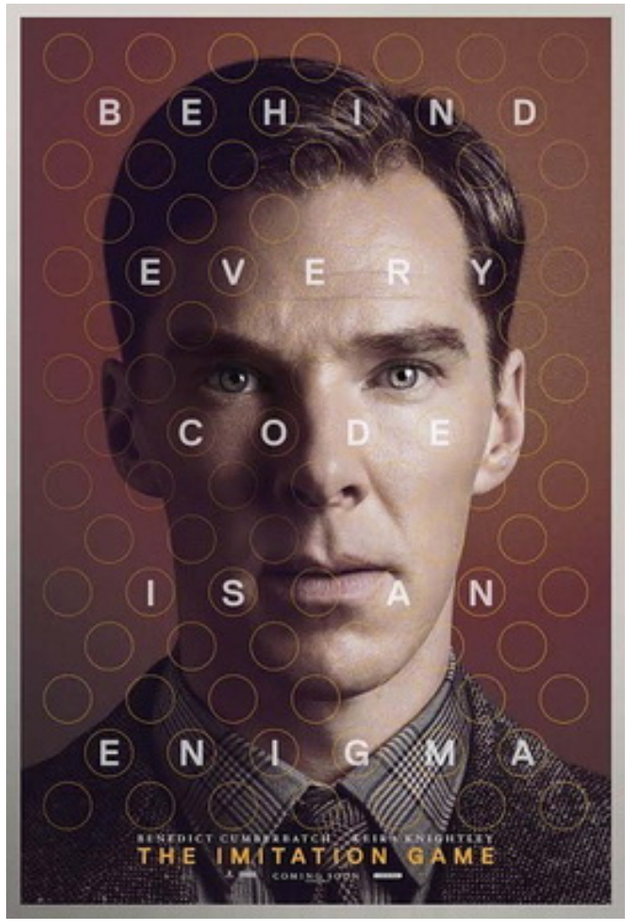
https://en.wikipedia.org/wiki/Alan_Turing

图灵

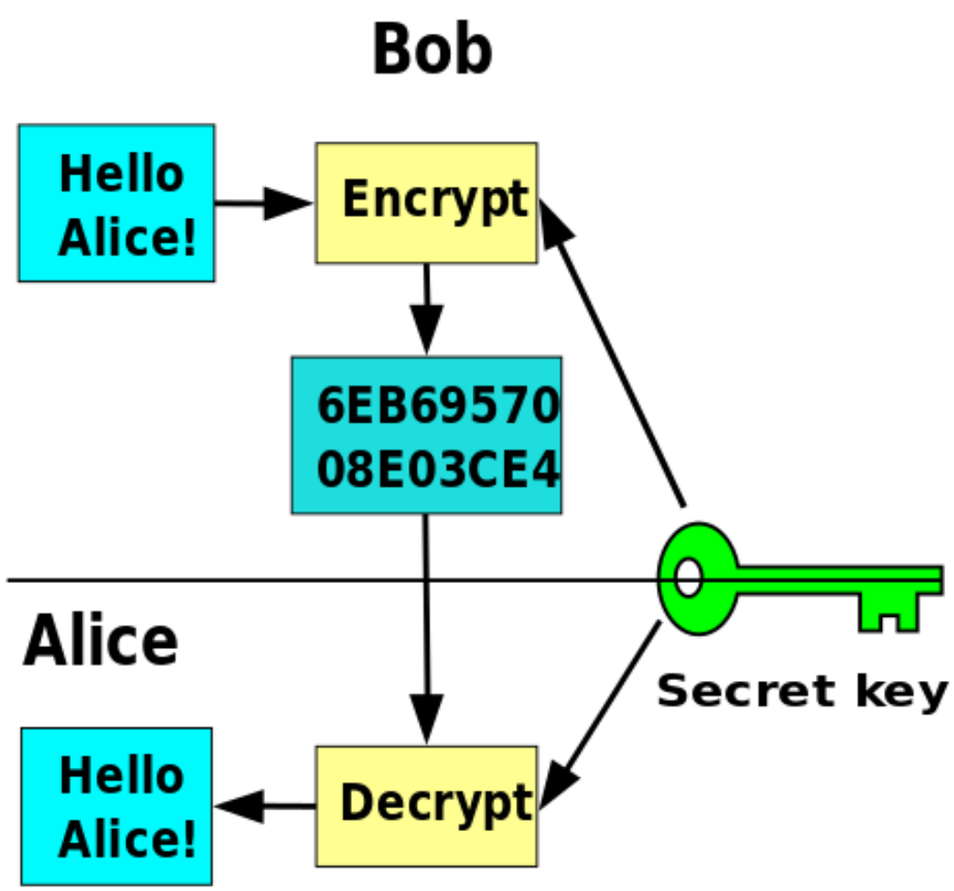


恩尼格玛密码机

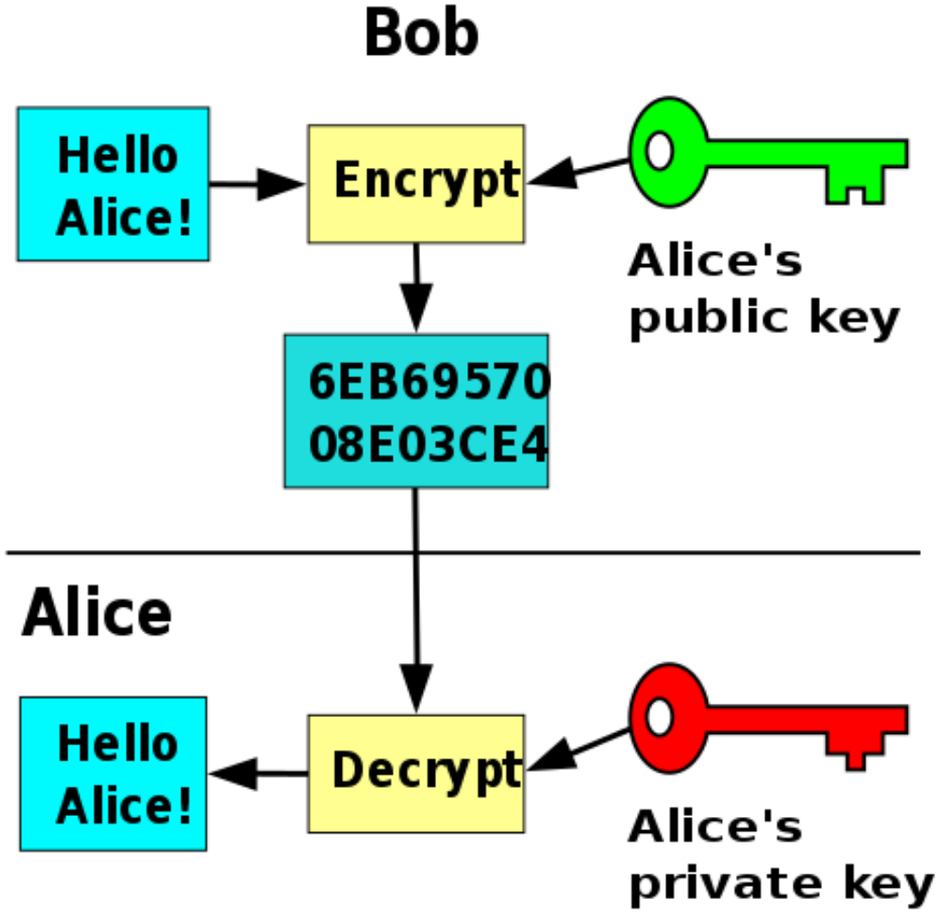
模仿游戏



对称密码学 vs. 非对称密码学



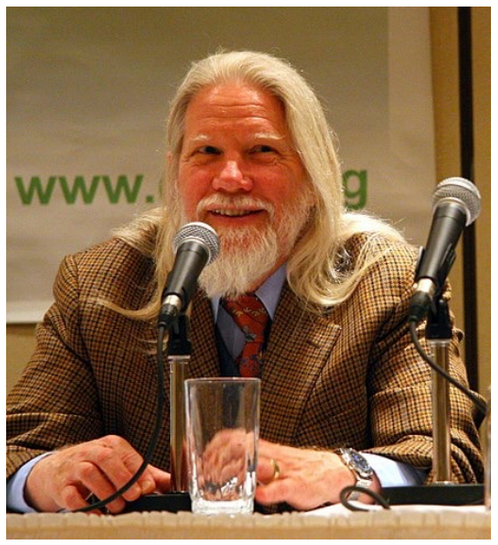
对称密码学



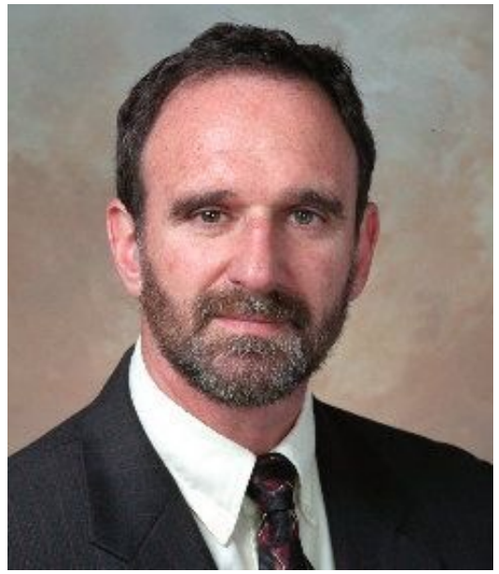
非对称密码学

DH vs. RSA

2015年
图灵奖



Whitfield Diffie



Martin Hellman

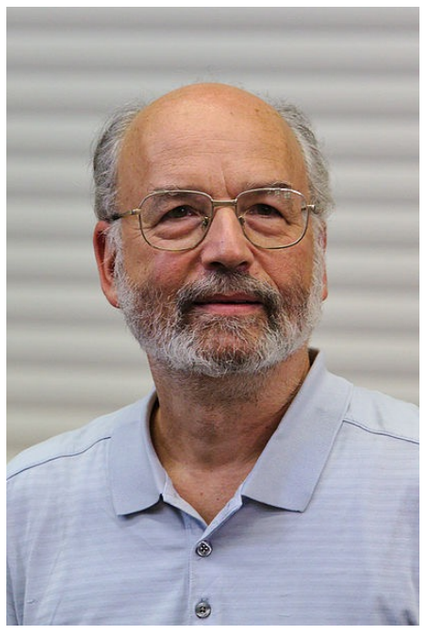
Ralph Merkle

1976

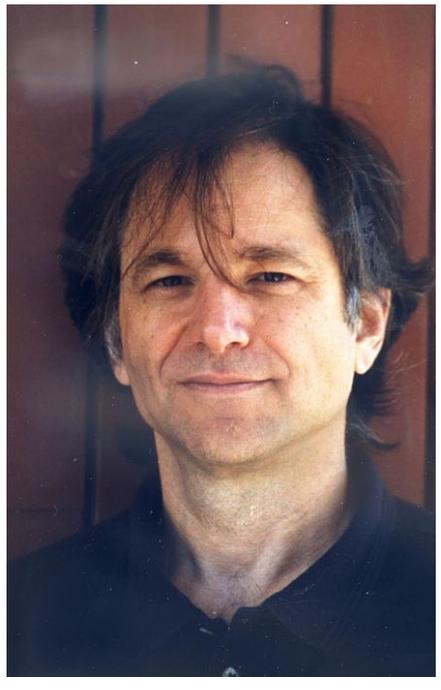
1978

2002年
图灵奖

Ronald L. Rivest



Adi Shamir

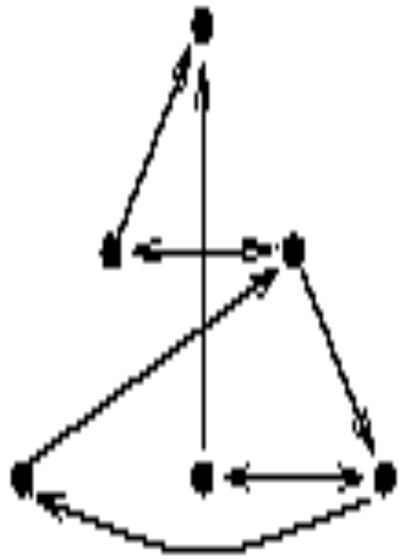


Leonard Max Adleman

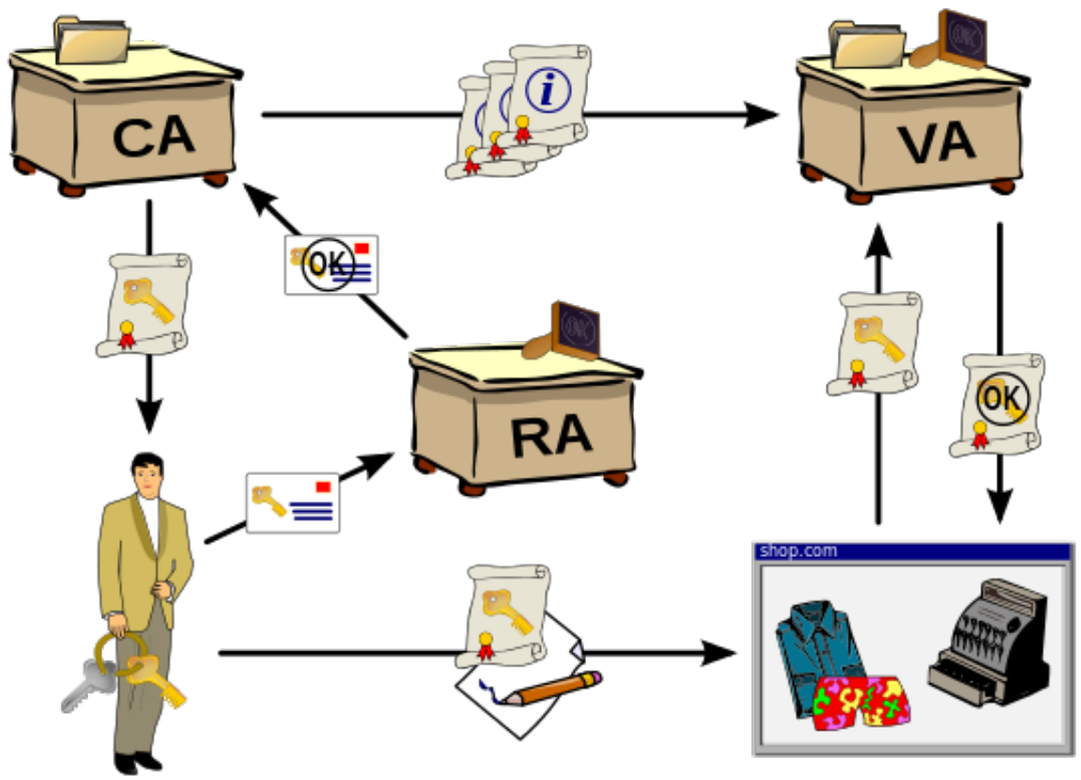
公钥管理: PKI vs. PGP

RSA

VERISIGN™



公钥管理的P2P版本



PGP®

1991

GnuPG

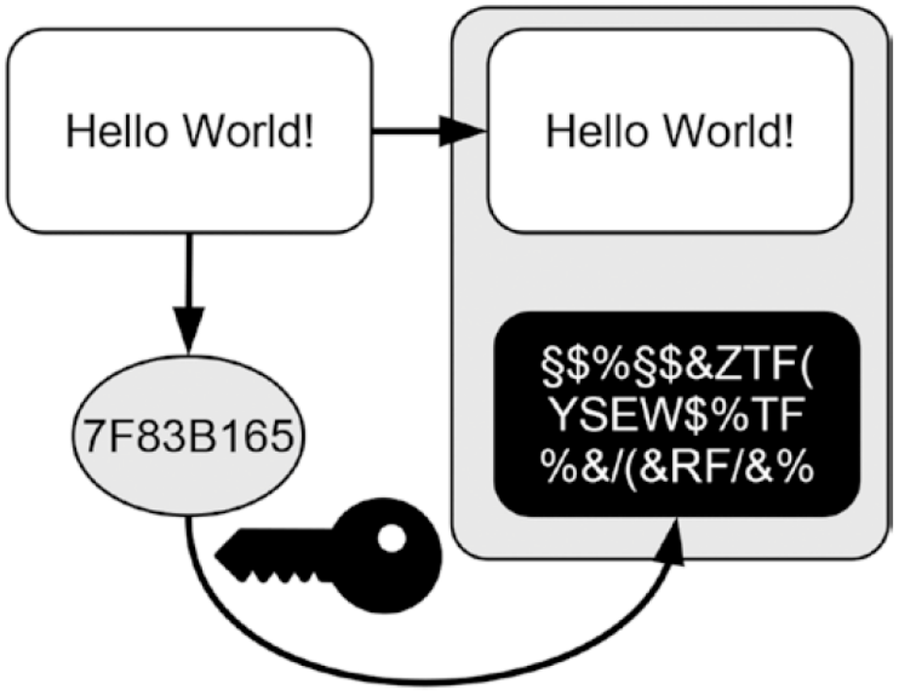
1999

Phil Zimmermann

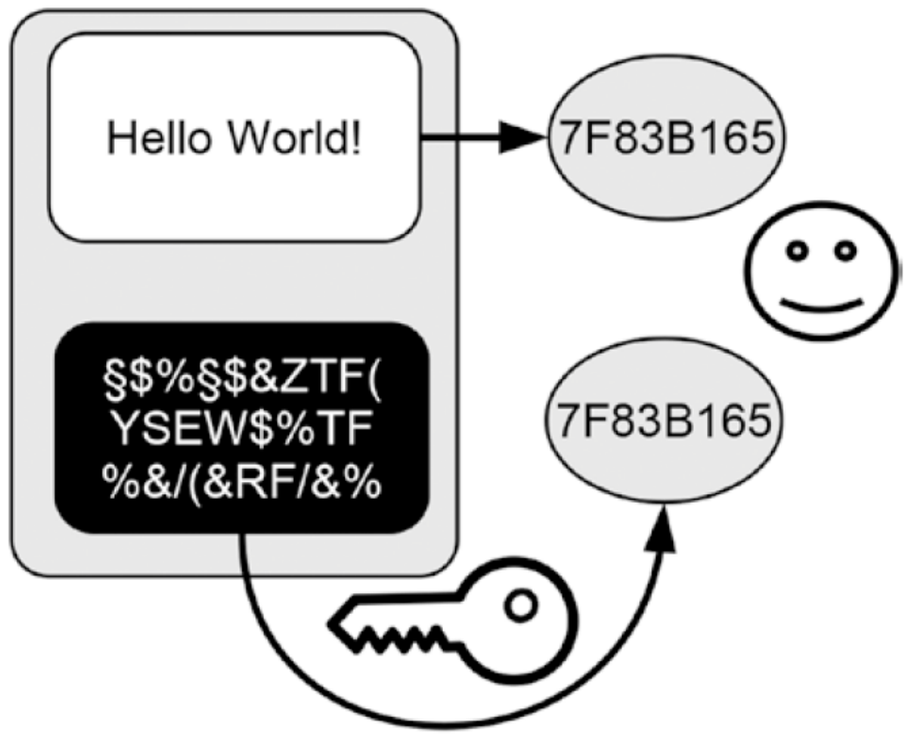
数字签名

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

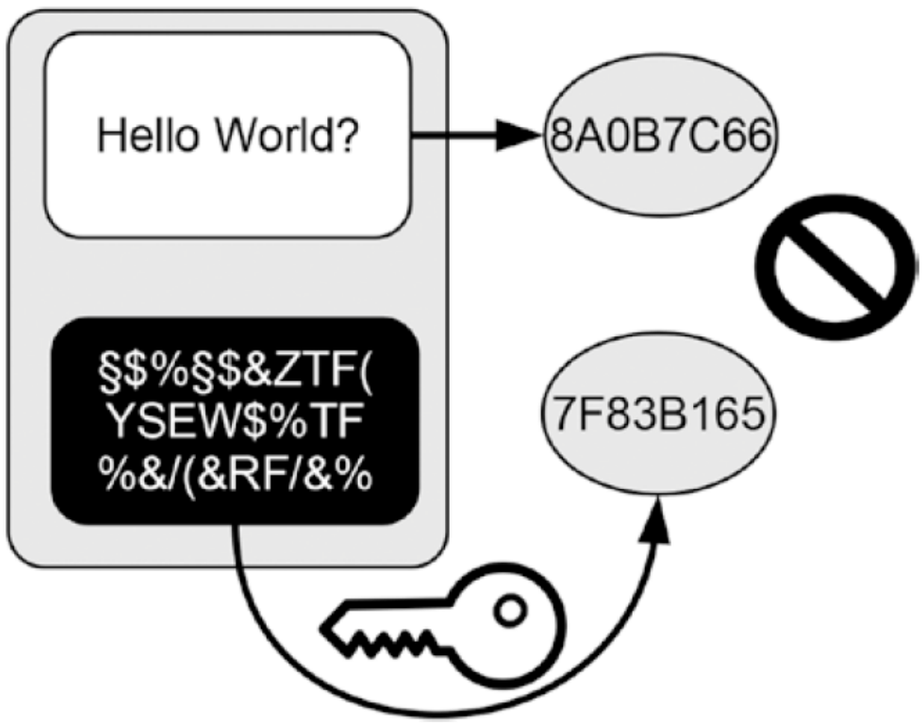
产生签名



验证签名



发现欺骗

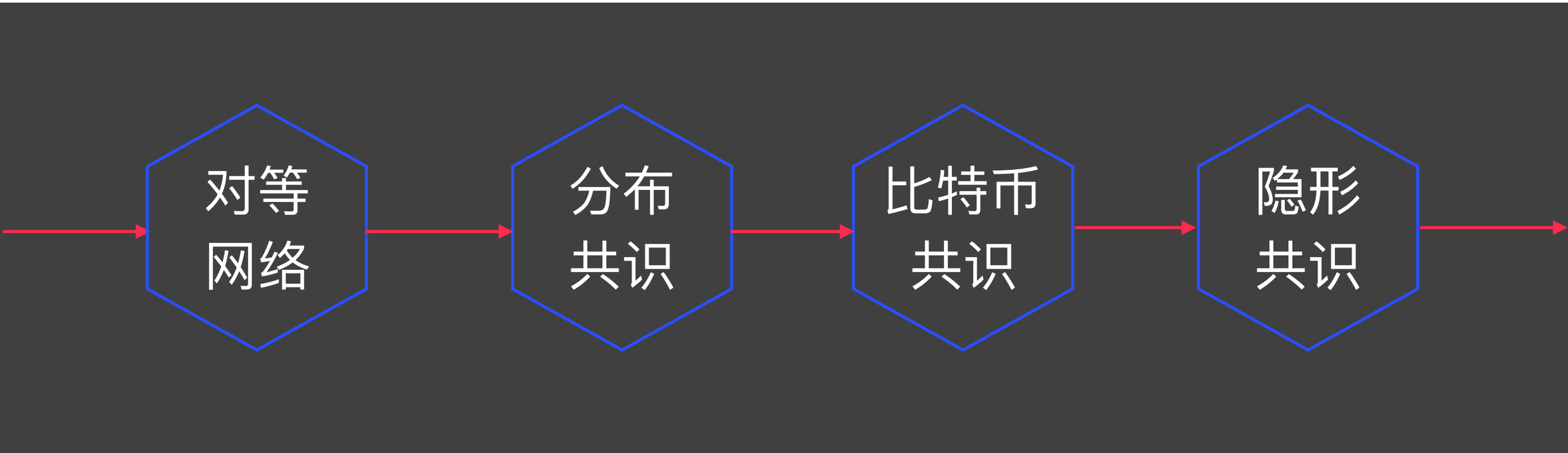


自己签名，任何人都可以验证（公钥分发）

不可伪造，公钥私钥

签名信息的大小

共识



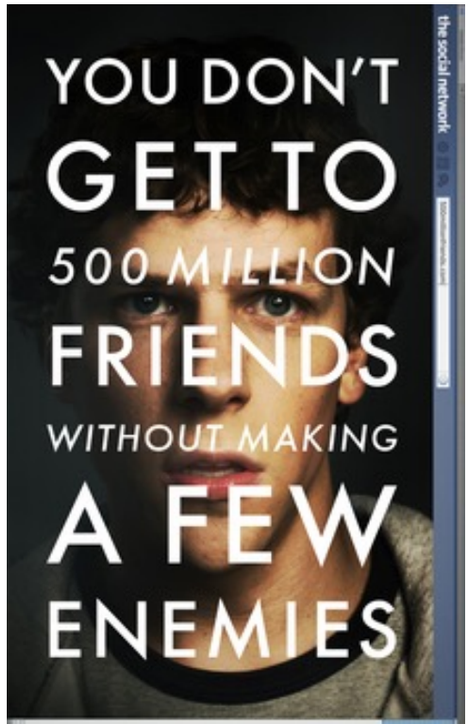
Peer to Peer

napster™

1999

Sean Parker

facebook



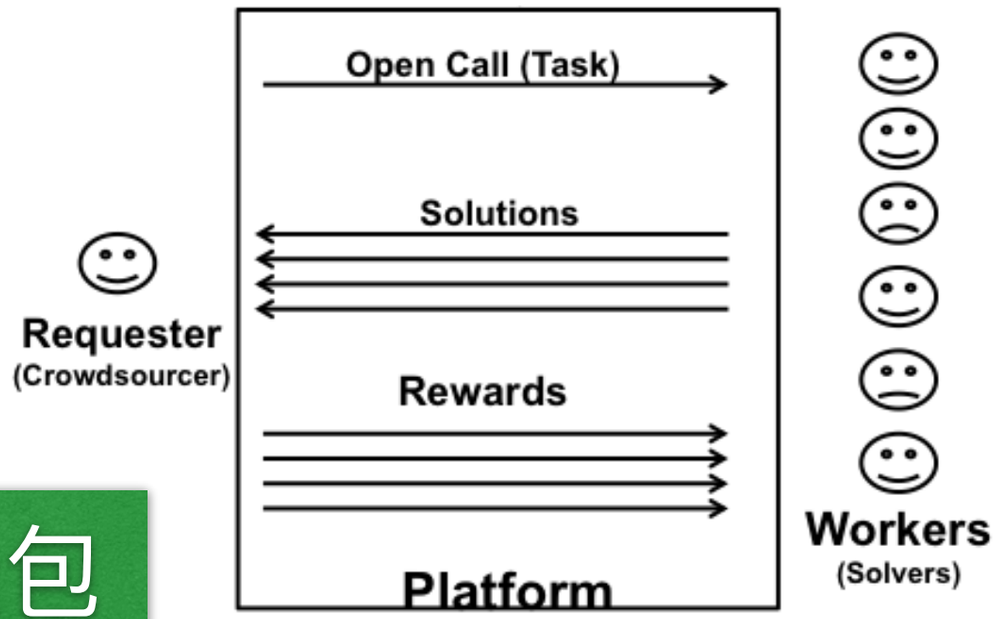
The Social Network

skype™

2003

KaZaA

众包



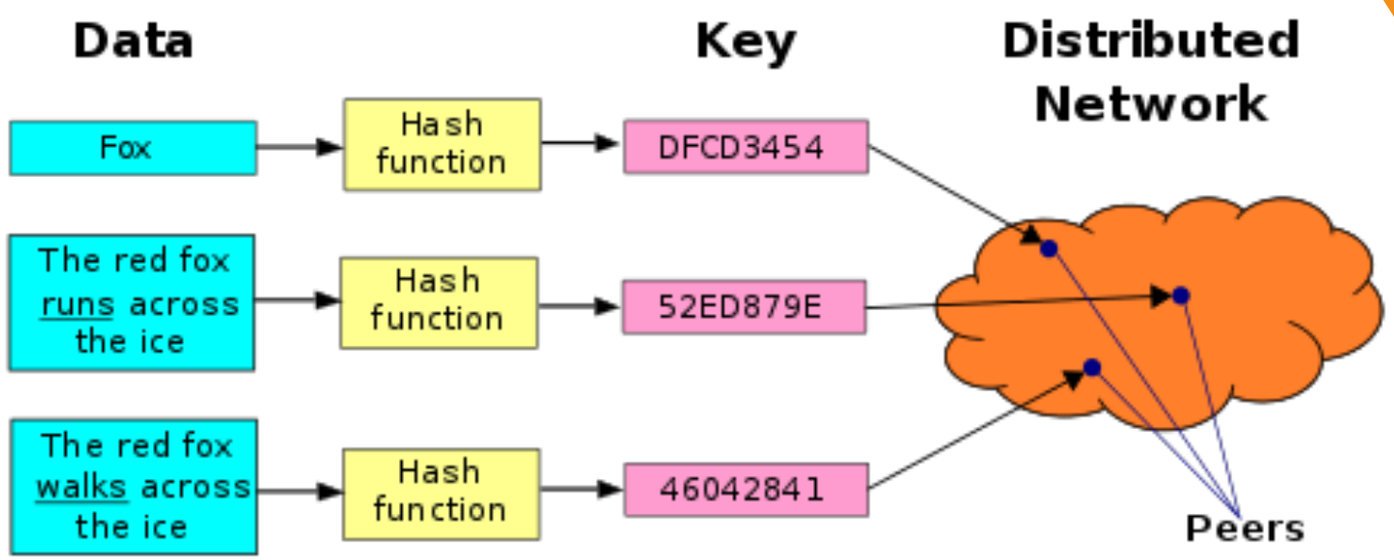
BitTorrent

2001

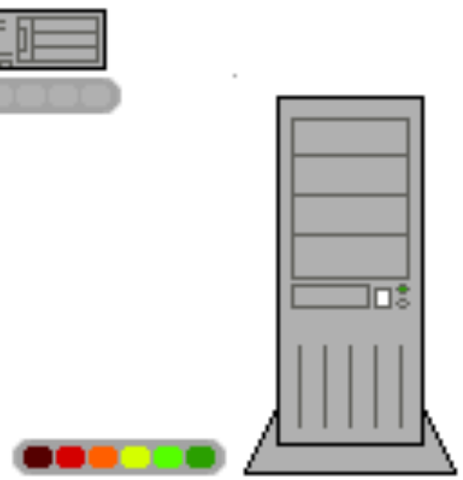
Bram Cohen

BitTorrent

Distributed Hash Table



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



激励

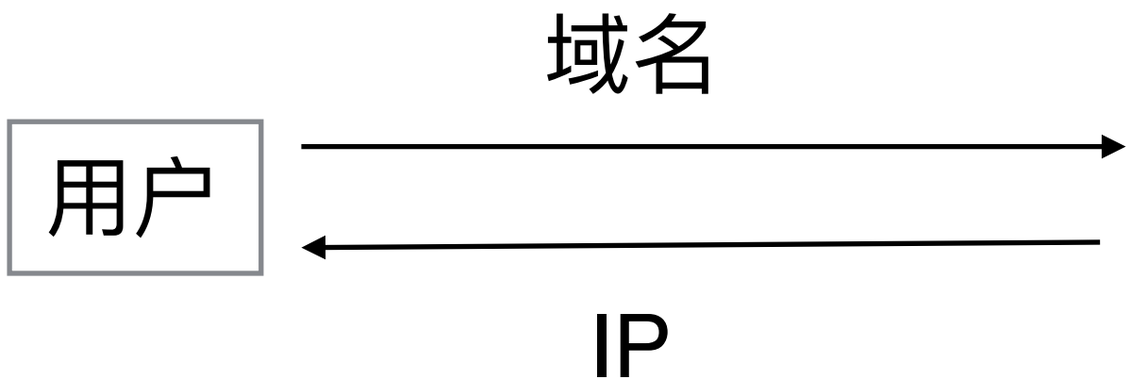
https://en.wikipedia.org/wiki/BitTorrent

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：

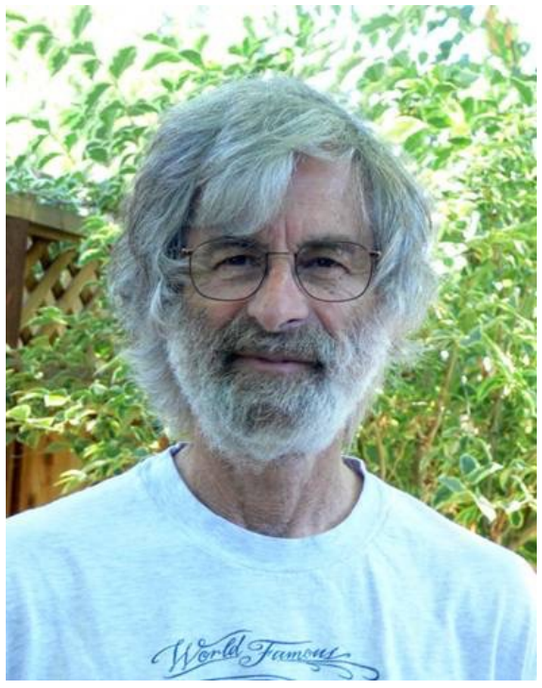
  ✳ 结束时所有诚实的节点均认同该值；

  ✳ 该值由诚实节点产生



Distributed DB, Email, PKI

拜占庭将军问题和Paxos



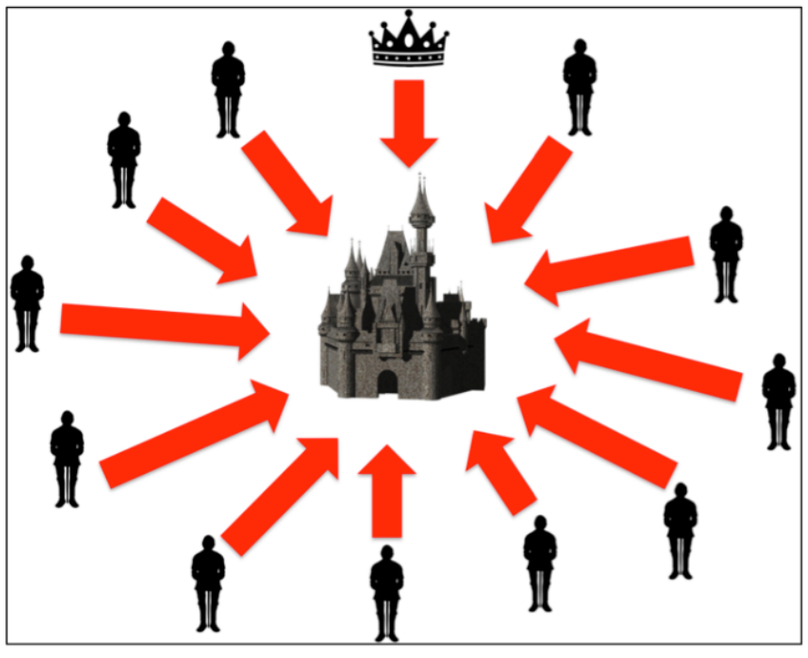
LESLIE LAMPORT

2013图灵奖

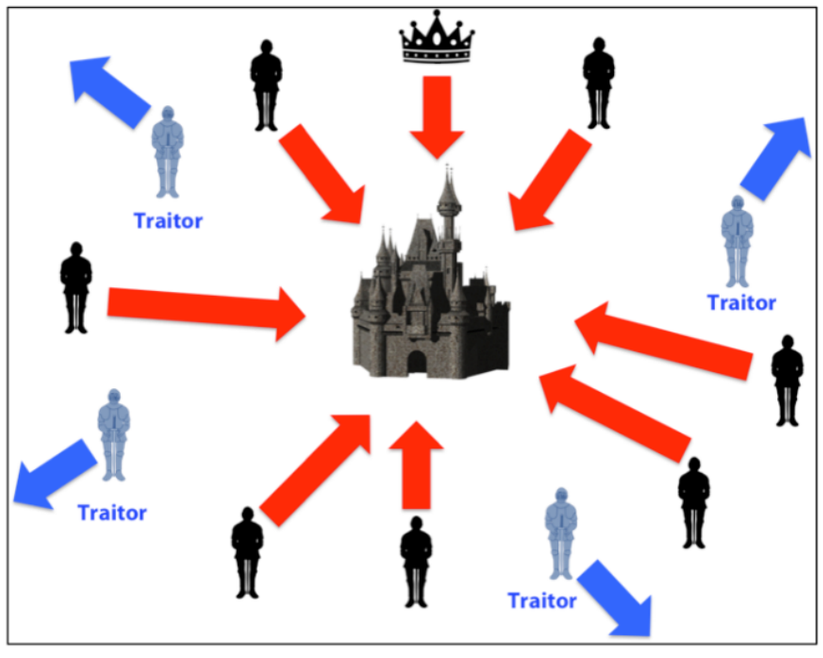
The Byzantine Generals Problem

1982

LESLIE LAMPORT, ROBERT SHOSTAK, and MARSHALL PEASE
SRI International



Coordinated Attack Leading to Victory



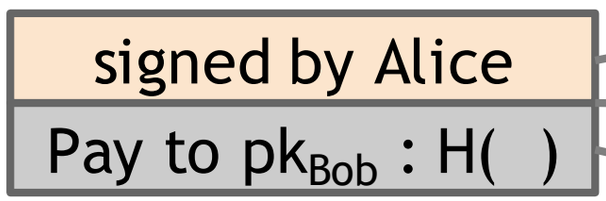
Uncoordinated Attack Leading to Defeat

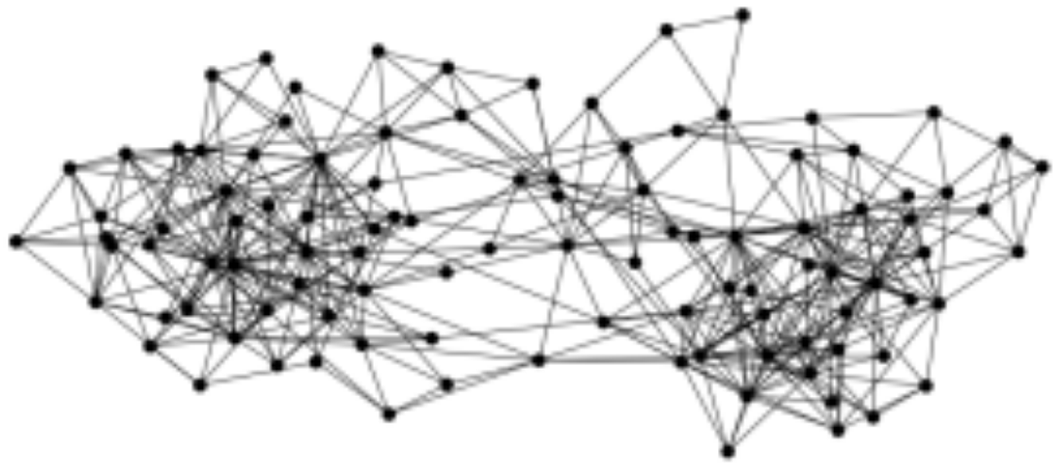
Paxos Made Simple

2001

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

比特币的交易传播

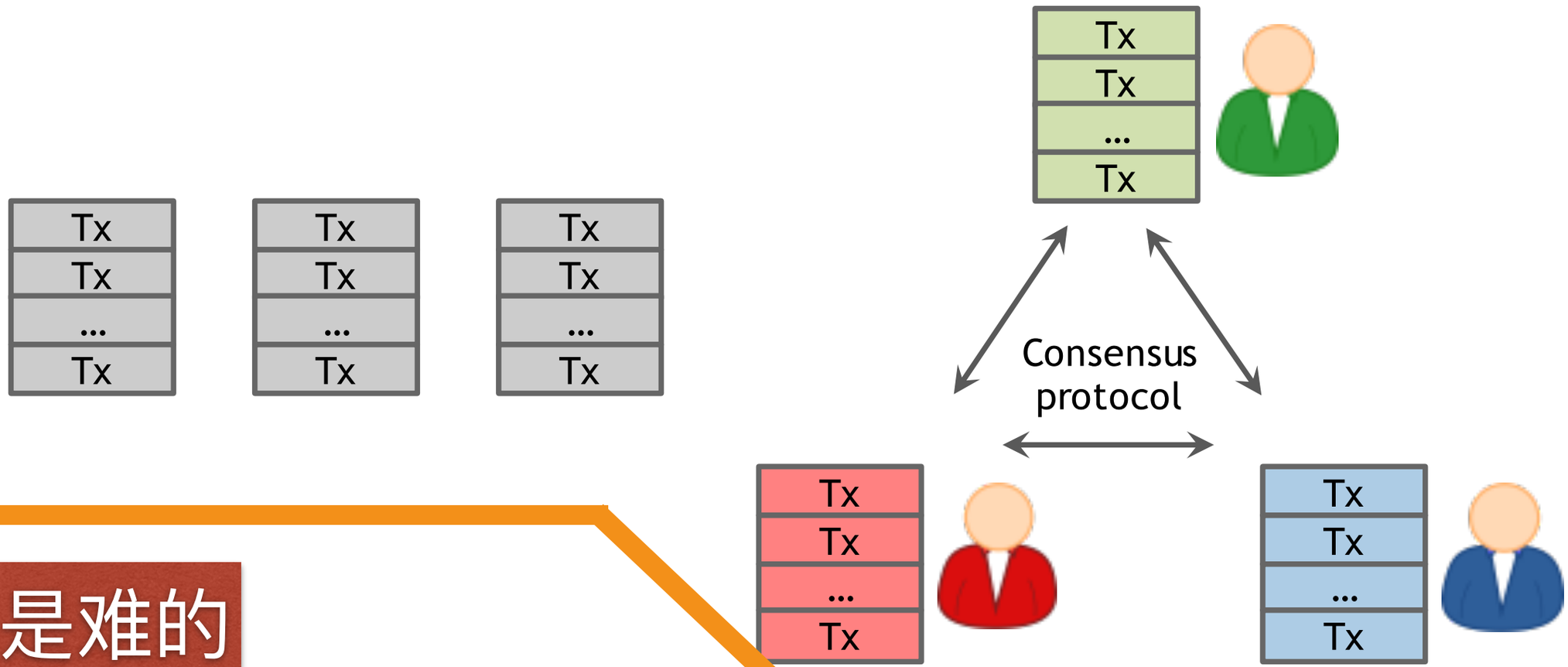




- 比特币是一个*P2P*网络
- *Alice* 需要广播她完成的交易給所有的节点
- *Bob*计算机当时可以不在*P2P*网络中
- *A single, global ledger for the system*
- 等待共识的业务、已共识的业务

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

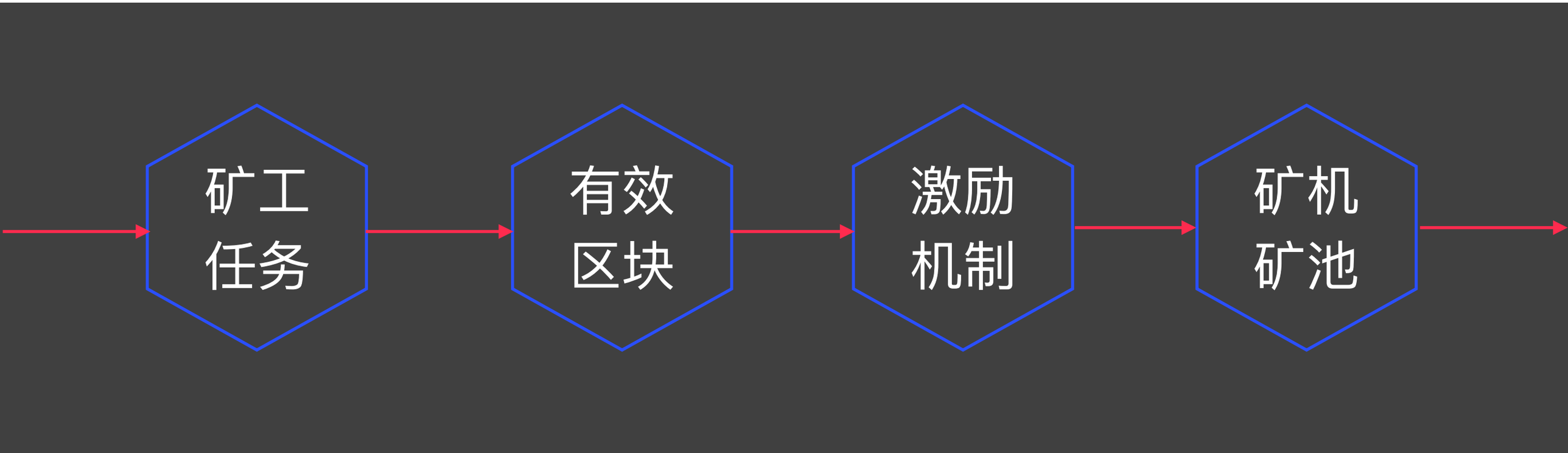
- 新的交易被广播到所有节点
- 每个节点将新的交易放进一个区块
- 在每一轮中，一个随机的节点被选择可以广播它的区块
- 其余节点可以选择接受这个区块，前提是区块的交易是可验证的
- 节点将以上区块的*Hash*放进自己的区块，表示它认可这个新区块

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

挖矿

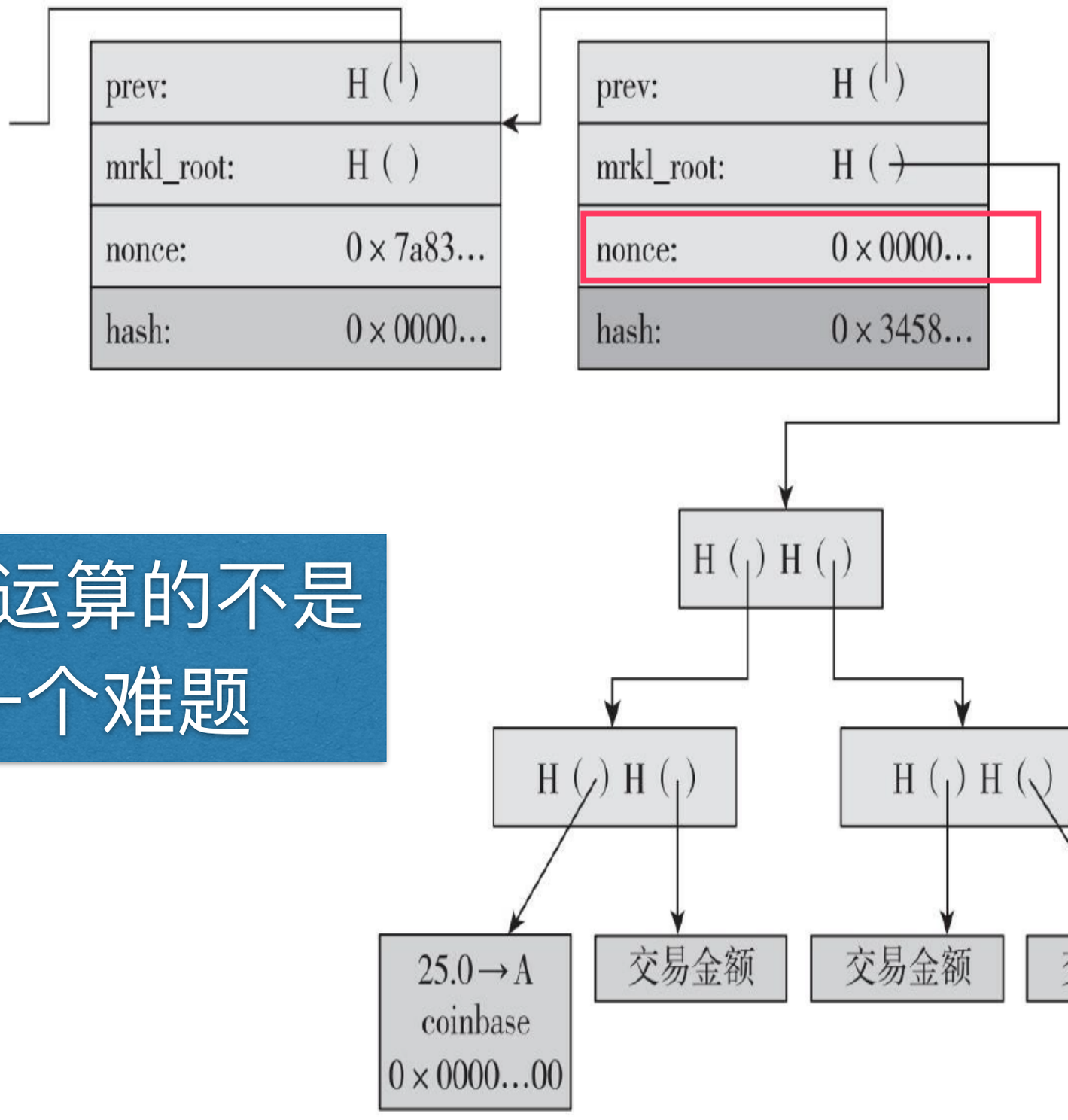


矿工的任务

- 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

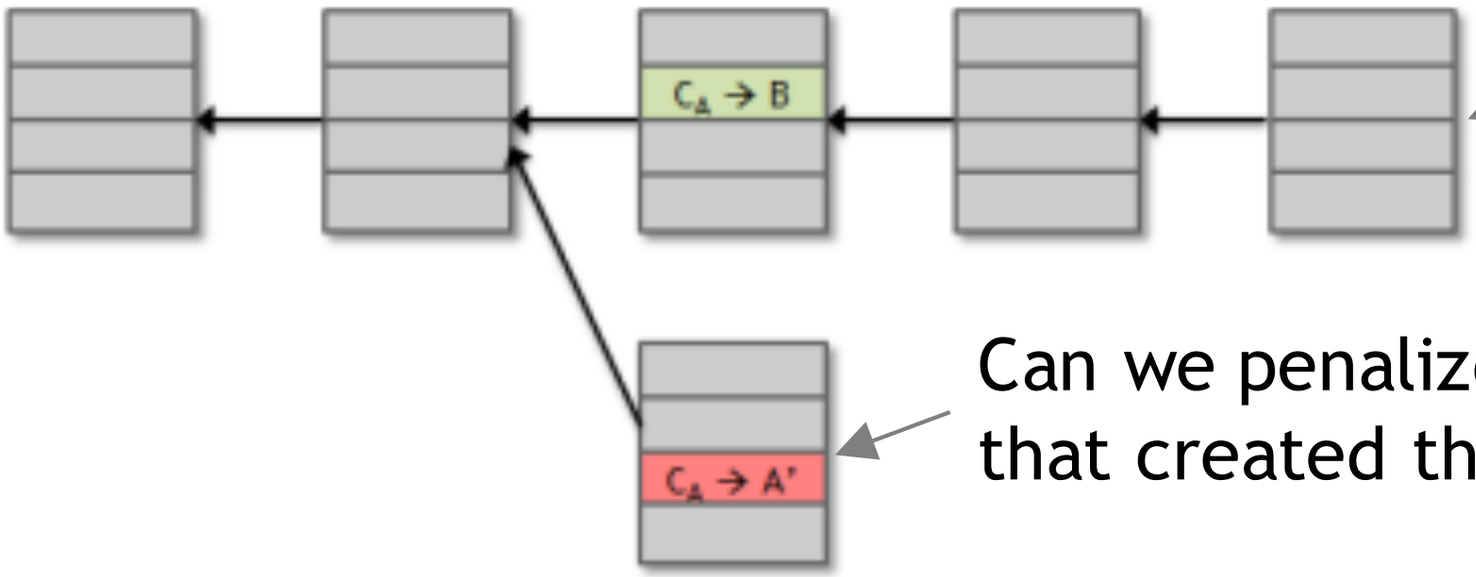
寻找有效区块



32位随机数

每个人运算的不是同一个难题

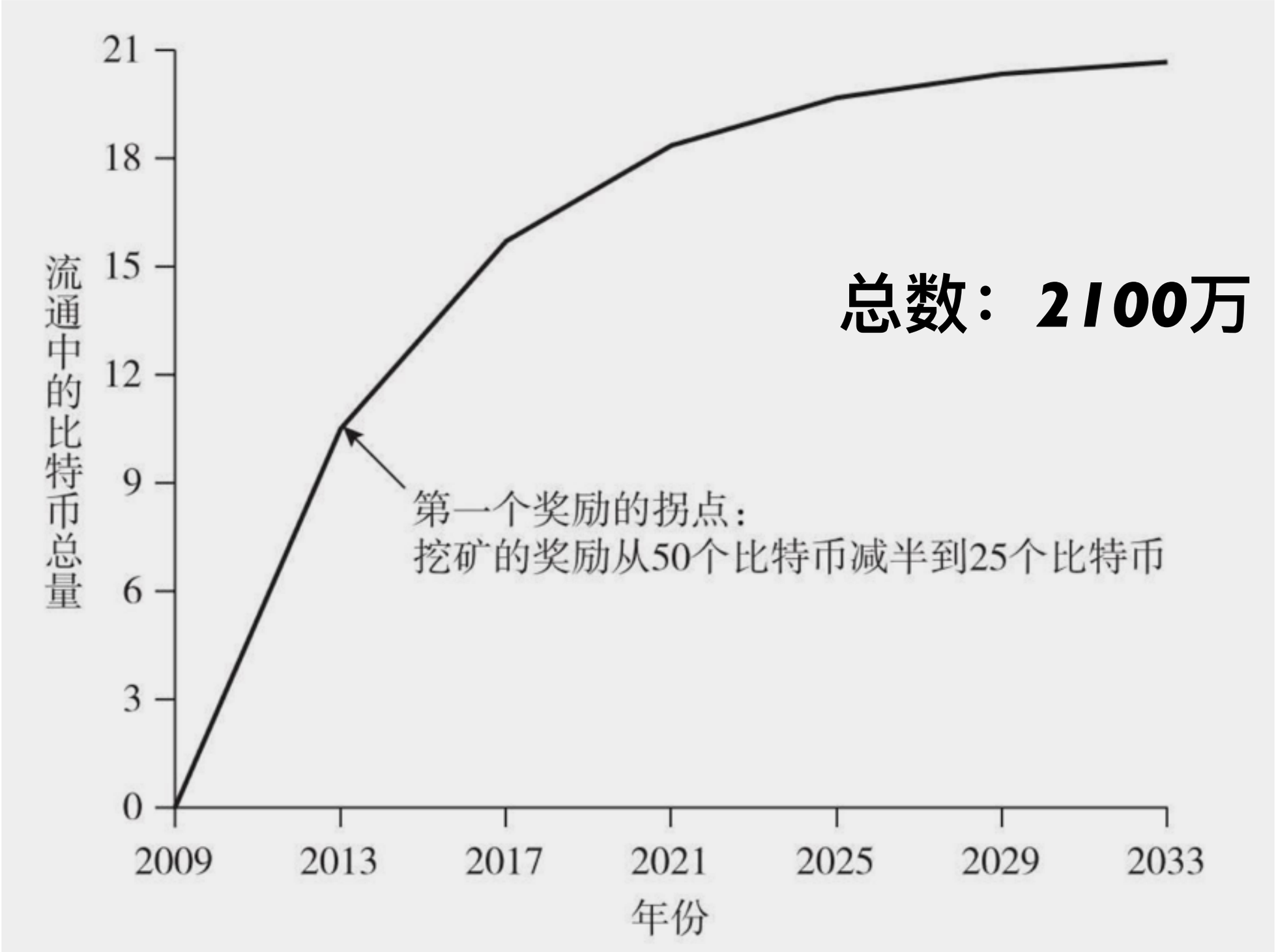
激励节点诚实



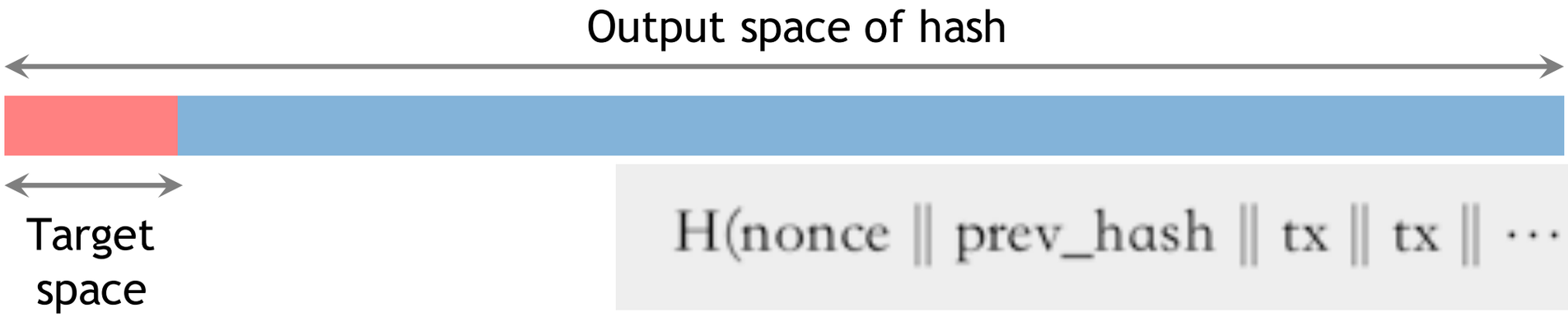
区块奖励 *vs.* 交易费奖励

交易费：输入和输出不等

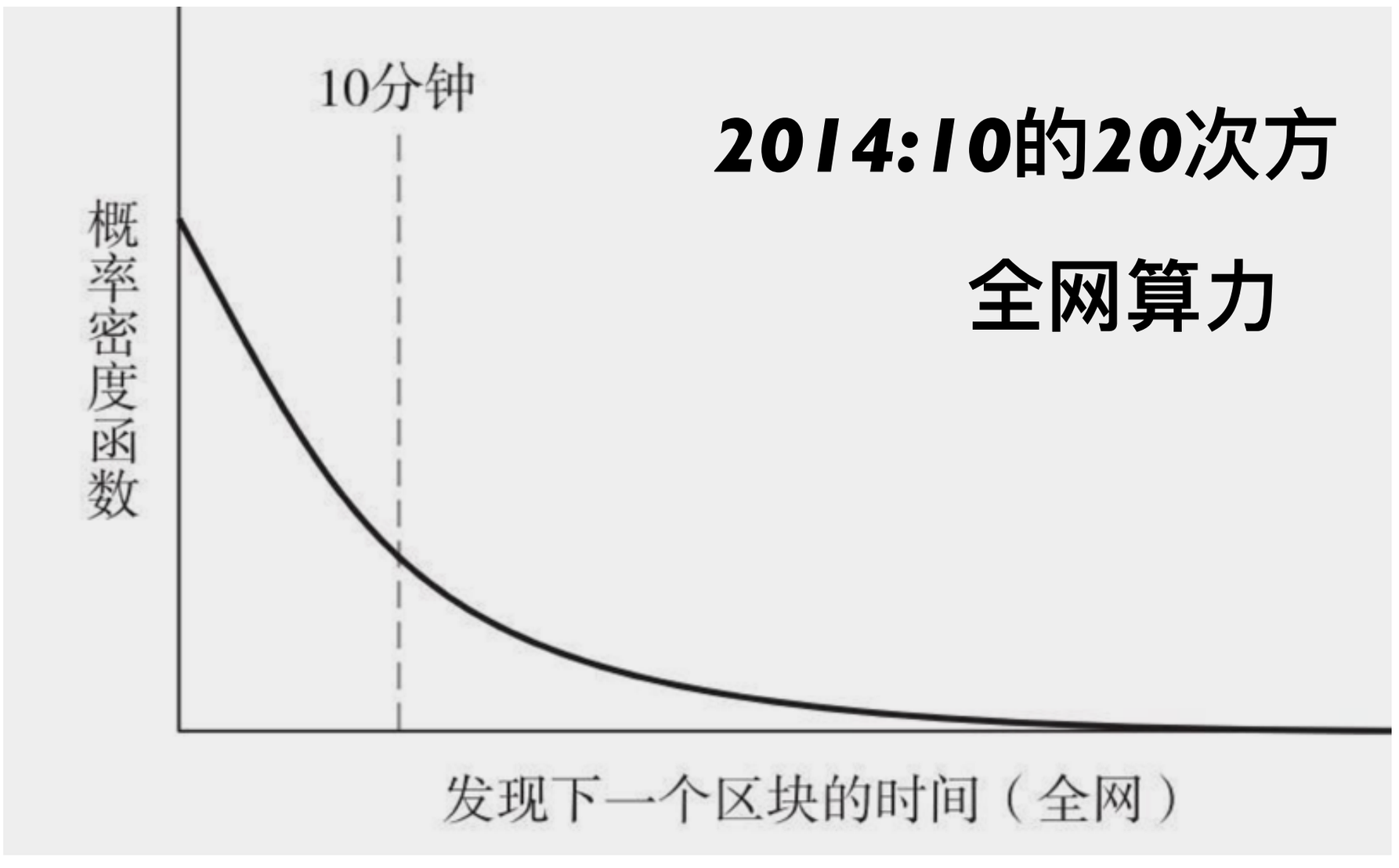
比特币奖励


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**

挖矿发展

CPU

GPU

FPGA

ASIC

gold pan

sluice box

placer mining

pit mining

Bitcoin01

专业矿场

温度

电费

网速

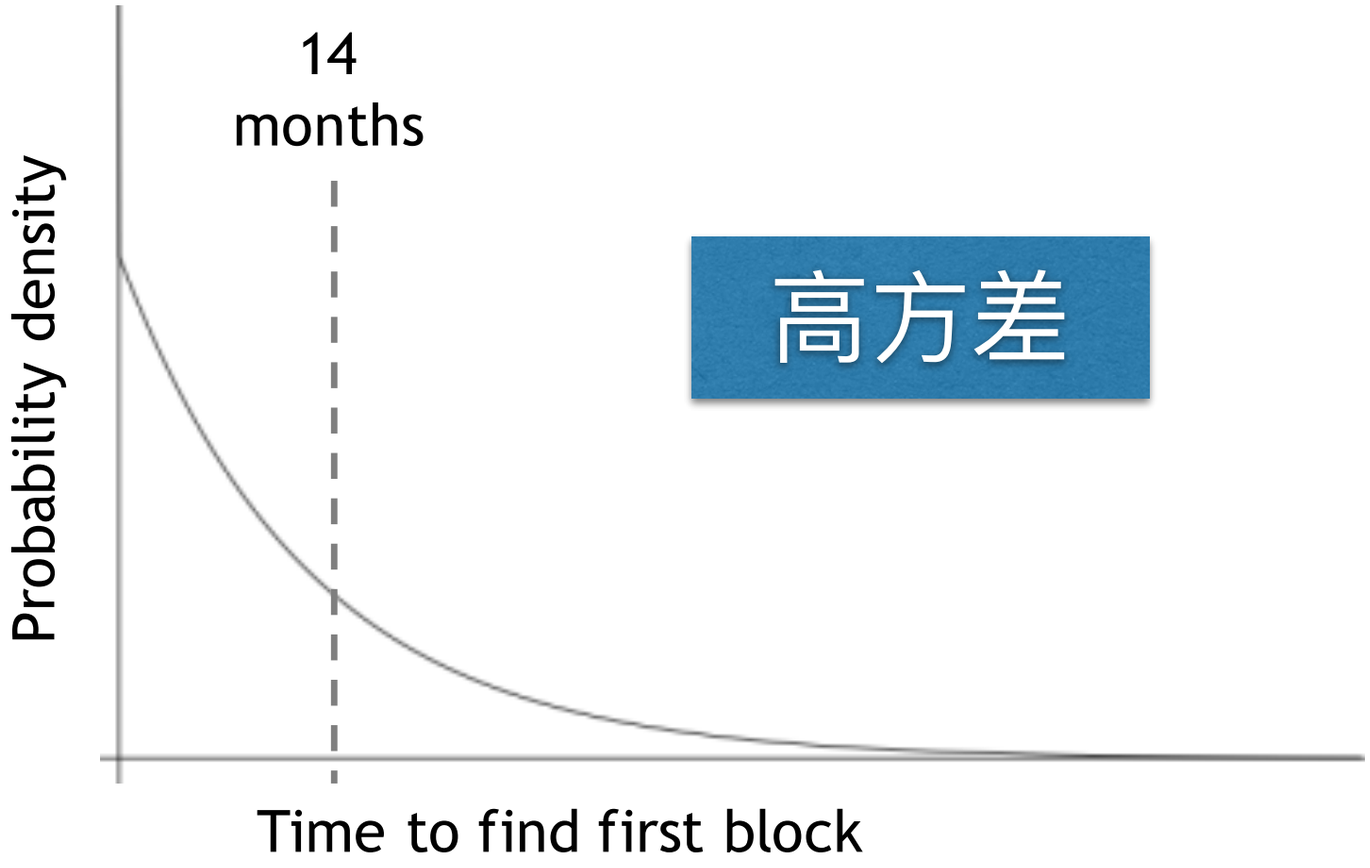
中国

矿池

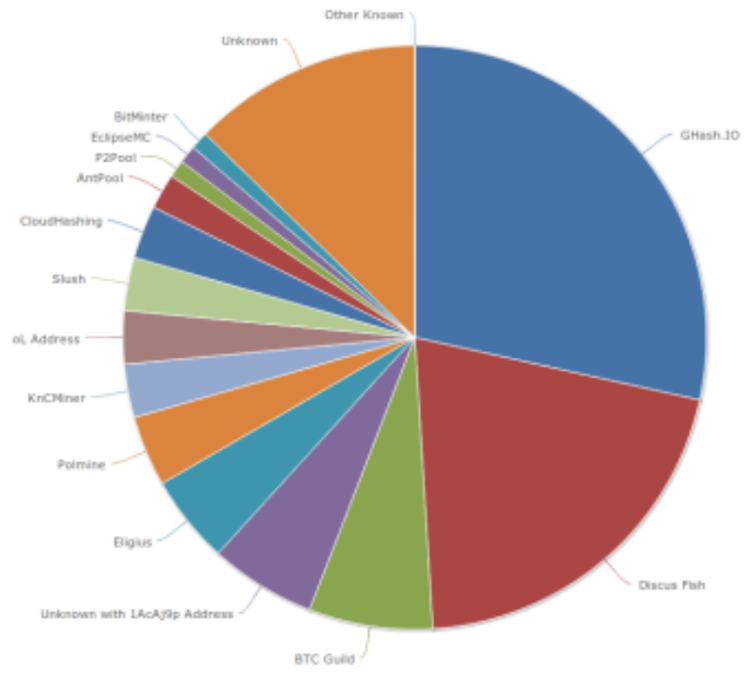
TerraMiner IV

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

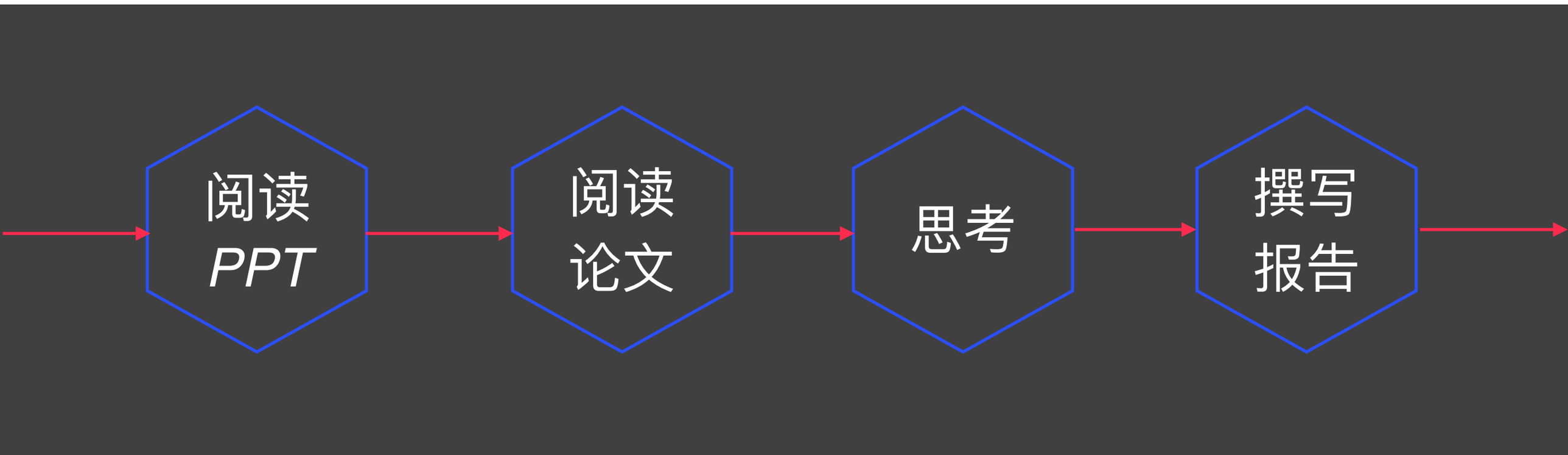
# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%



高方差



课后作业



谢谢！

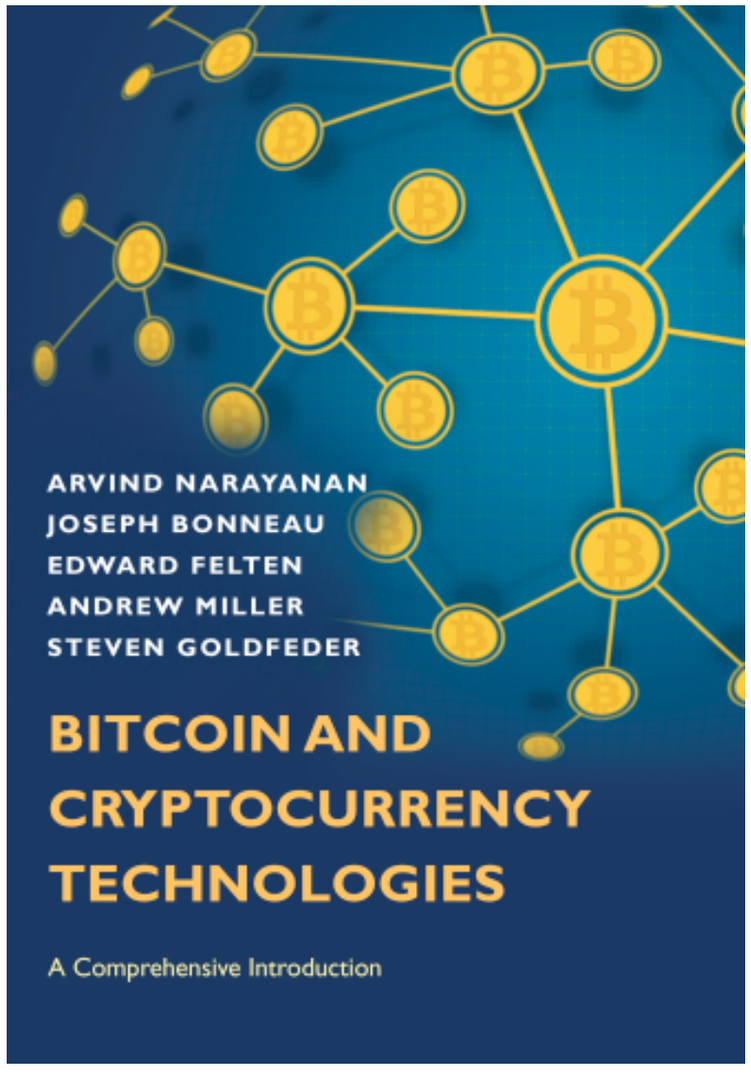
Huiping Sun

sunhp@ss.pku.edu.cn

https://huipingsun.github.io

Homework

阅读教材



阅读引言

阅读第1-5章

Homework

课后作业

要求阅读如下资料，写阅读报告

Bitcoin Developer Guide

Find detailed information about the Bitcoin protocol and related specifications.

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

1、资料概述

2、主要收获

3、存在疑问

4、所思所感

周日晚上12点前
提交给助教