



2023.02.28

比特币 -01



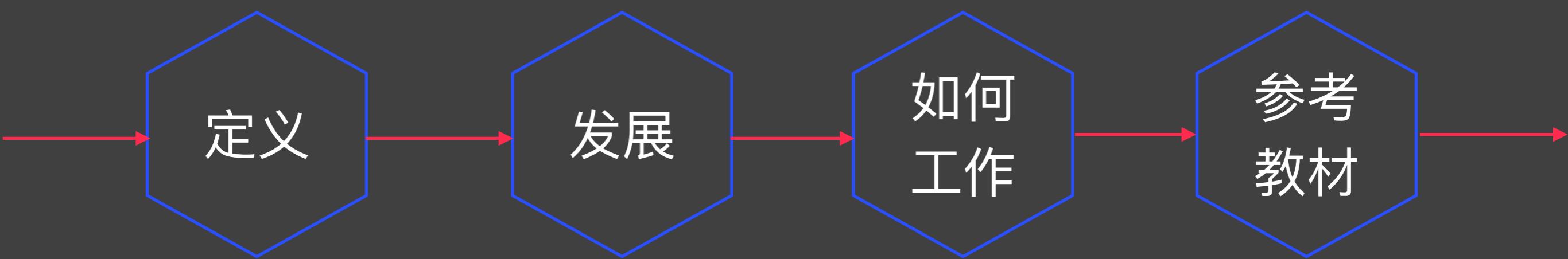
上次课程内容回顾



本次课程内容



简介



比特币是一个创新的支付网络，一种新的货币。

比特币网络中参与者存储和传输的货币单位

bitcoins

Bitcoin

构成数字加密货币生态基础概念技术的总称

基于P2P，无需中央管理机构，去中心化

开源软件，设计公开，任何人无法控制

快速端到端交易，随时随地可用，交易媒介

跨境支付便捷，手续费低，身份隐私受保护

Bitcoin

比特币历史价格

比特币历史价格走势图

默认为今年以来的价格(单位: 美元)

<https://history.btc123.fans/>

月 季度 半年 YTD 年 所有

开始时间 2010-05-22 结束时间 2023-02-26

最高市值
2.2万亿美元

当前市值
4500亿美元

2021.11
68789

50000

2011.02
1

2013.04
100

2017.11
10000

2021.03
60000

2023.02
23594

2010.07
0.1

2012.08
10

2013.12
1000

2011

2012

2013

2014

2015

2016

2017

2018

2019

2020

2021

2022

2023

月 季度 半年 YTD 年 所有

开始时间 2010-05-22 结束时间 2013-02-21

2010.05
比特币披萨
25美元
1万个比特币

大涨
60多倍

MT.Gox
黑客事件

30

20

10

0.025

2010-07

2010-10

2011-01

2011-04

2011-07

2011-10

2012-01

2012-04

2012-07

2012-10

2013-01

Bitcoin

比特币历史价格

比特币历史价格走势图

默认为今年以来的价格(单位: 美元)

月 季度 半年 YTD 年 所有

开始时间 2012-12-19 结束时间 2017-03-16



默认为今年以来的价格(单位: 美元)

月 季度 半年 YTD 年 所有

开始时间 2017-03-16 结束时间 2023-02-03



比特币影响力



服务热线: 95566 信用卡热线: 40066 95566

首页

公司金融

个人金融

银行卡

金融市场

电子银行

当前位置: 首页 > 关于中行 > 媒体看中行

全球数字货币市值3891亿美元，已超美国银行、富国银行市值 【第一财经】

2018-03-29

https://www.bank-of-china.com/aboutboc/ab8/201803/t20180329_11873775.html

截至2018年3月10日，全球数字货币种类超过1500种，
合并市值高达3891亿美元。
已超过美国银行3018亿、富国银行2492亿市值
市值排名第一的比特币市值占比高达41.3%

全球逾半数中央银行正在探索或开发数字货币



2022年7月

- 启动 (2)
- 试点 (15)
- 概念验证 (15)
- 研究 (65)



来源: CBDC Tracker (cbdctracker.org)。

注释: 该地图同时显示了零售型和批发型央行数字货币。一个国家可以有多种央行数字货币; 该地图显示了每个国家央行数字货币最先进的发展阶段。地图上显示的边界、颜色、名称和任何其他信息并不表示IMF对任何领土的法律地位所做的评判或对此类边界的认可或接受。

<https://www.imf.org/zh/Publications/fandd/issues/2022/09/Picture-this-The-ascent-of-CBDCs>

IMF: 加密货币不应被授予法币地位，有必要制定和应用全面法规

2023年2月23日

<https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092>

货币历史



商品货币时代

- 货币价值主要取决于贵金属的发现和冶炼

信用货币时代

- 货币本身没有价值而取决于对发行机构的信任

去中心货币时代

- 货币价值取决于人们对算法、系统的认可



Bitcoin P2P e-cash paper

Satoshi Nakamoto Sat, 01 Nov 2008 16:16:03 -0700

I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.

The paper is available at:
<https://www.bitcoin.org/bitcoin.pdf>

The main properties:

- Double-spending is prevented with a peer-to-peer network.
- No mint or other trusted parties.
- Participants can be anonymous.
- New coins are issued from a timestamp style proof-of-work.
- The proof-of-work for new coin generation also powers the network to prevent double-spending.

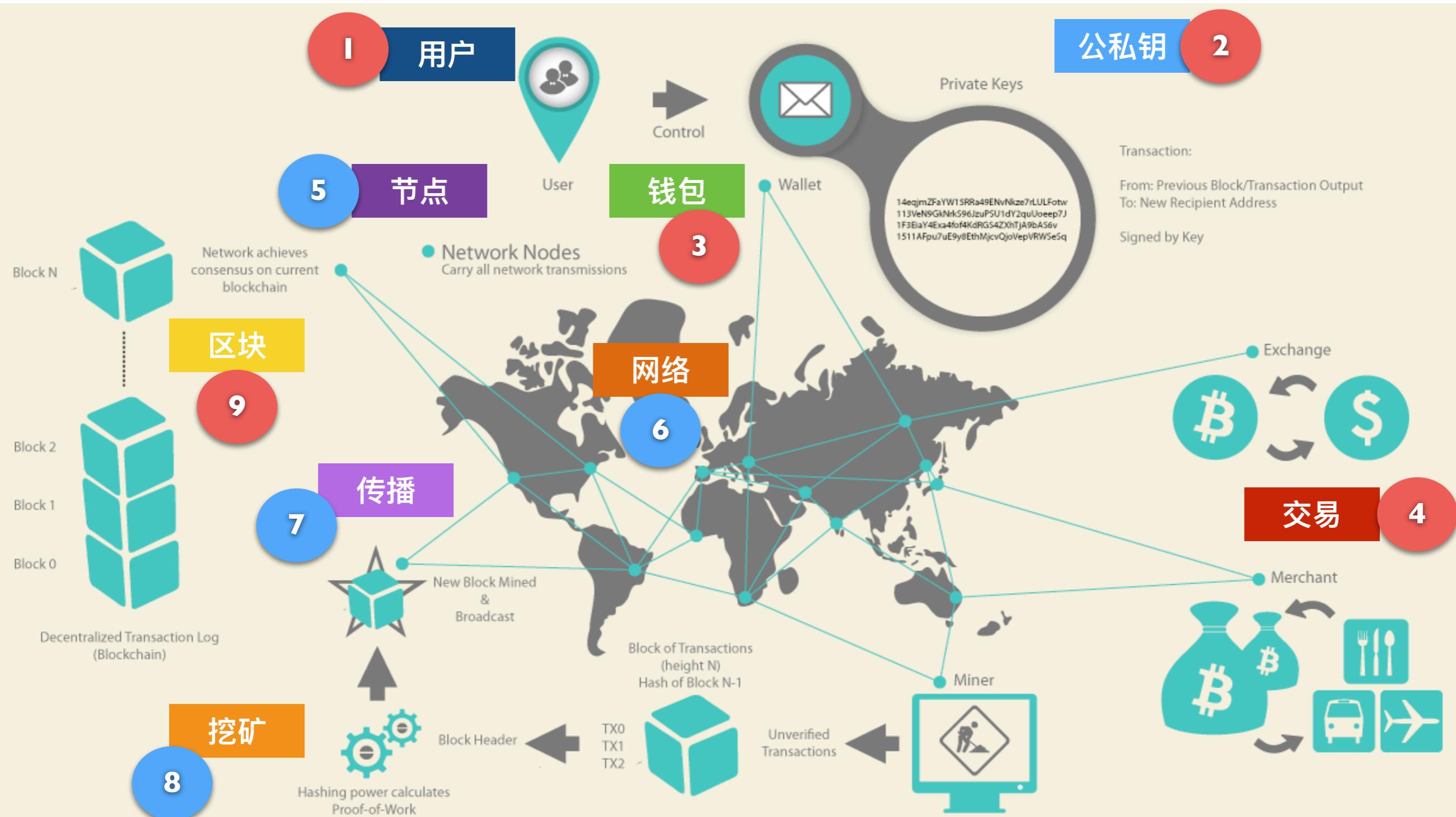
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the need for an中间人 (middleman) or financial institution. Digital signatures provide part of the solution, but most of the benefits are lost if a trusted party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by having them include the timestamp of the previous transaction in the chain. This allows the network to prevent double-spending without relying on a central authority or trust. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of power. As long as honest nodes control the majority of CPU power on the network, they can generate the longest chain and outpace any attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Full paper at:
<https://www.bitcoin.org/bitcoin.pdf>

Satoshi Nakamoto

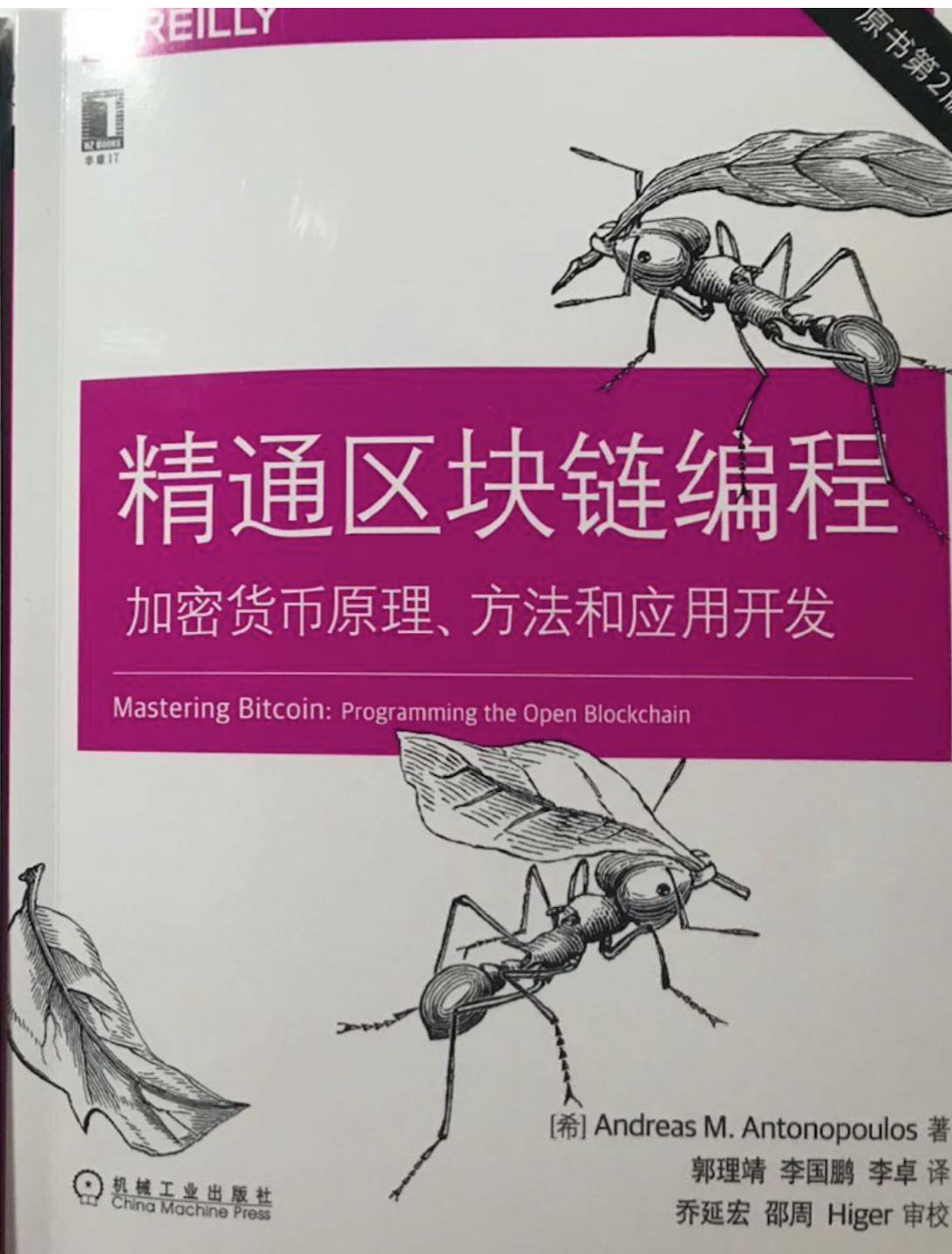
The Cryptography Mailing List
 Unsubscribe by sending 'unsubscribe cryptography' to

比特币如何工作

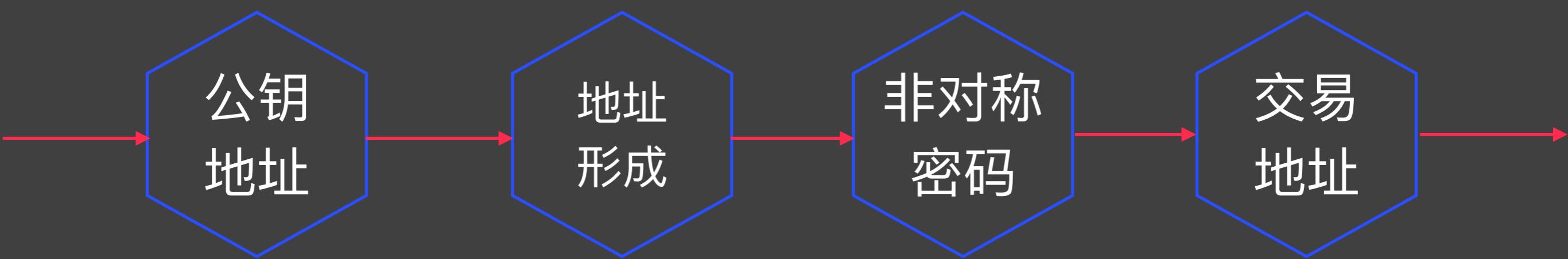


Bitcoin

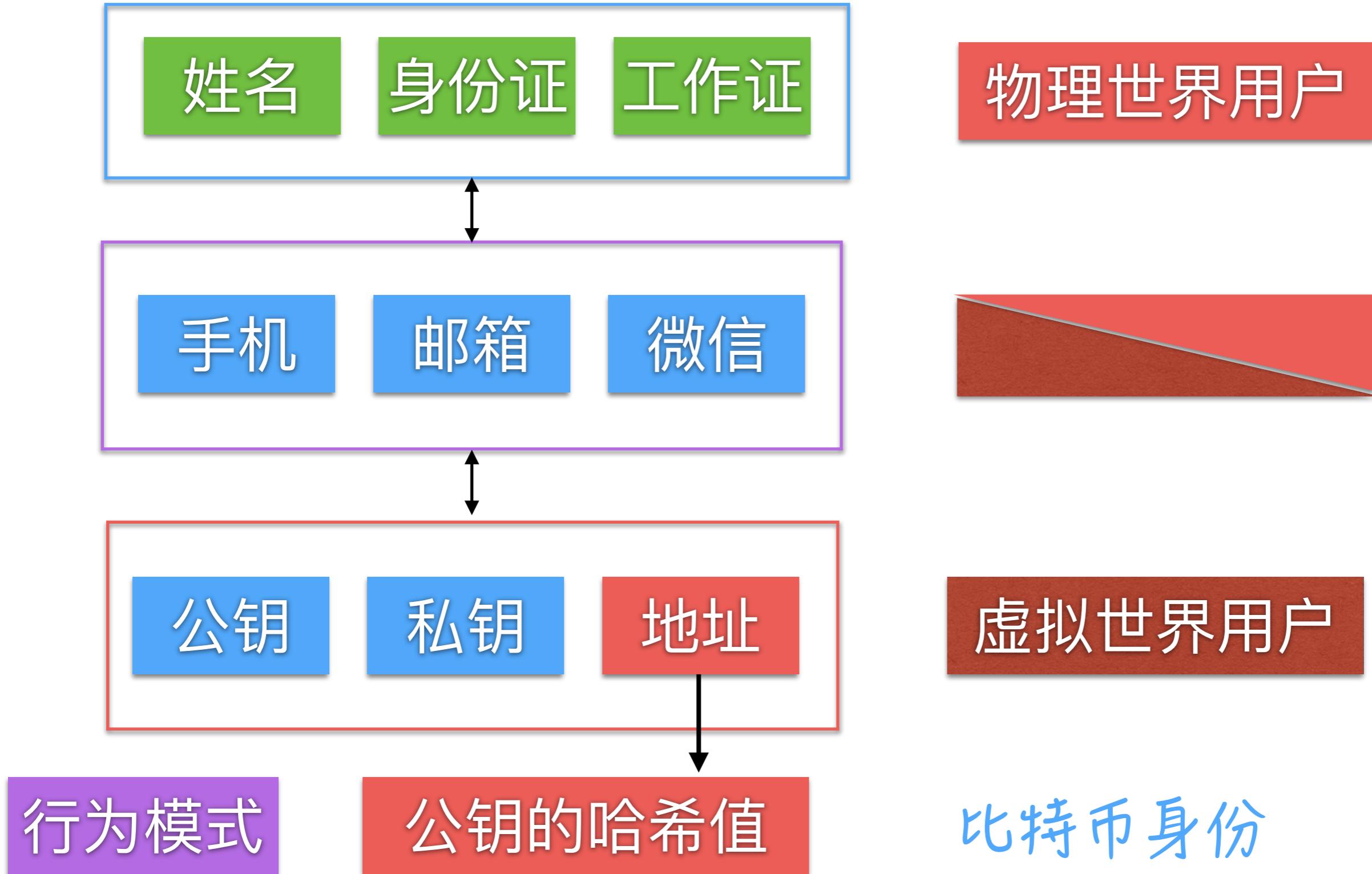
《Mastering Bitcoin》



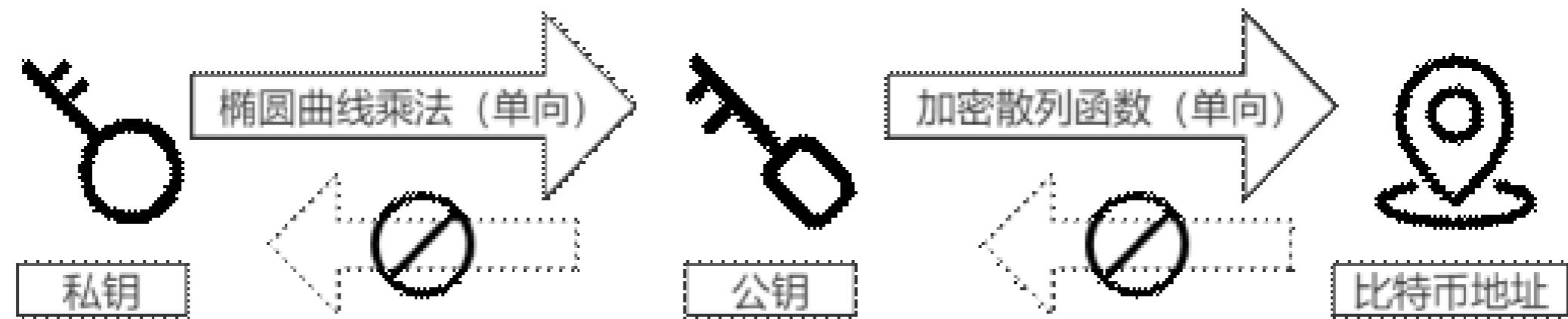
地址



身份



私钥、公钥、地址



私钥

2ScXxzUJasEibnzD3DKBKyoMQdhmsiXR9mCi97pEMfzPLdzdZVuEgt

公钥

WIF压缩

02b234135dbd947c3d39285a0e9cfbacfcfc79a799a9aa9c7155dab0cf0948c88e

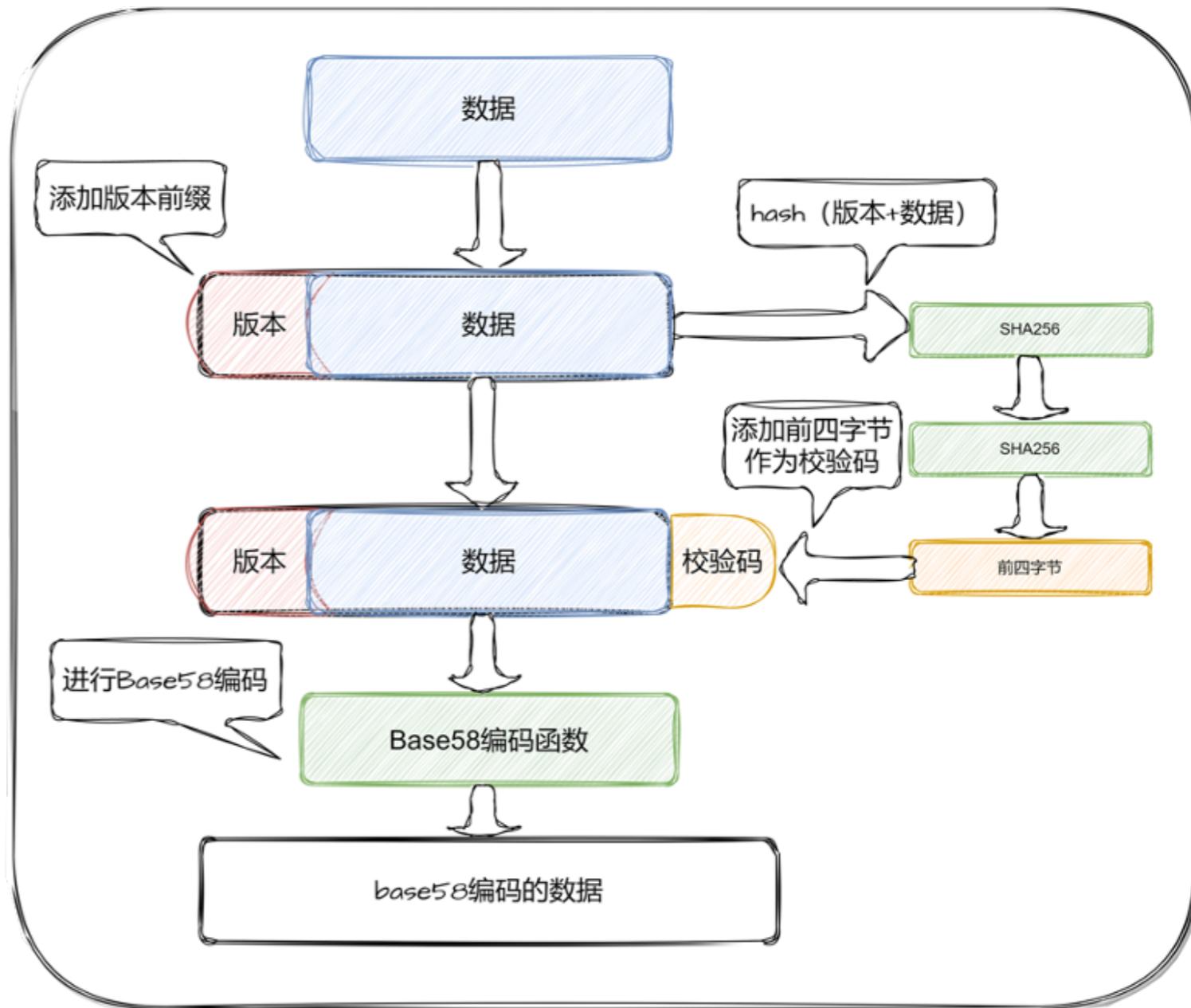
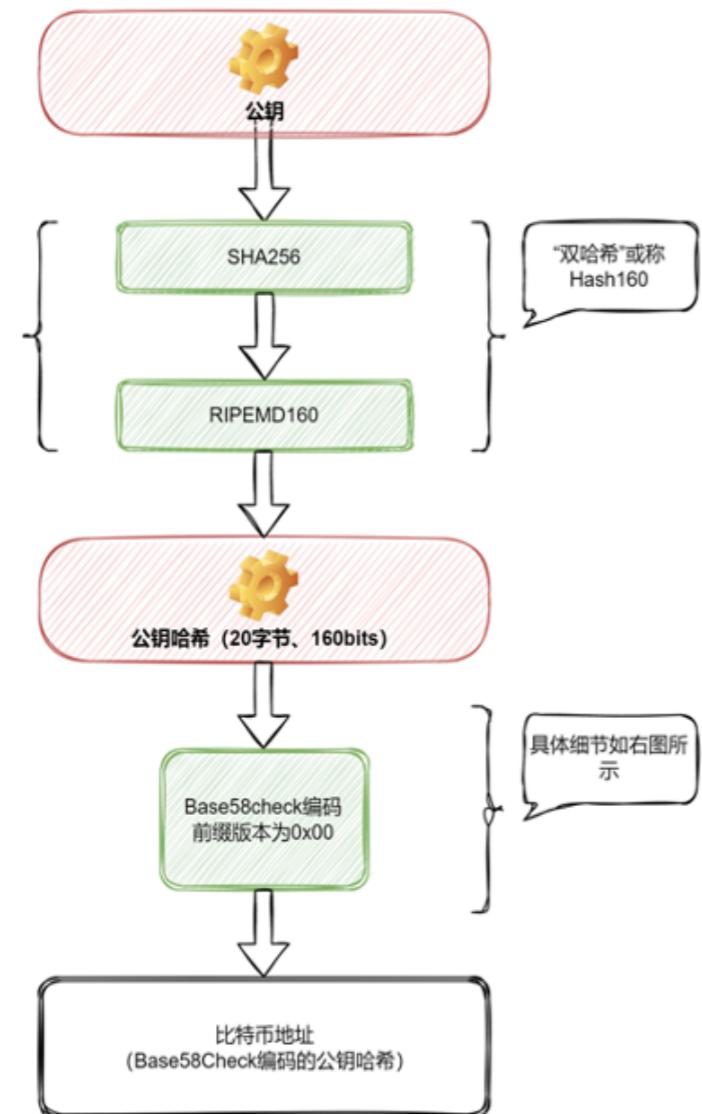
地址

压缩Hex

17hWhVByis35z9vmFgLv3gMbKtYZ2f5zZZ

BTC

公钥到地址



Base64

大写字母
小写字母

数字
+、 /

Base58

0和○
1和I

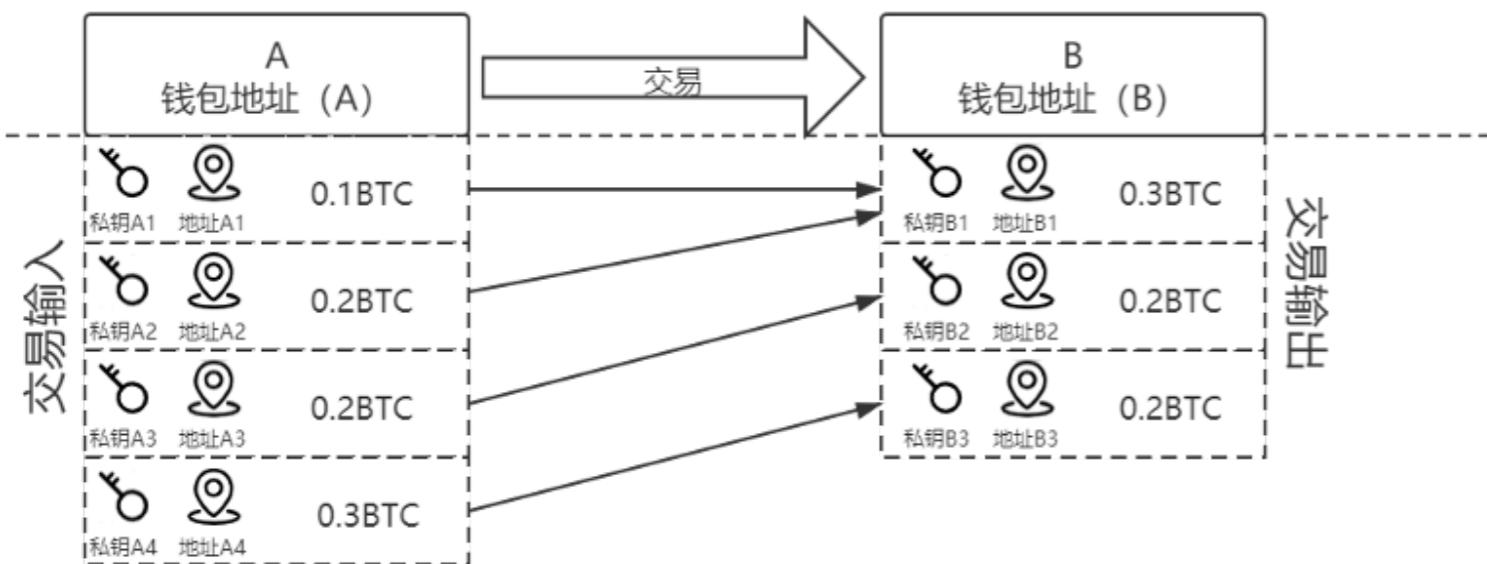
Base58
Check

检验和

交易地址



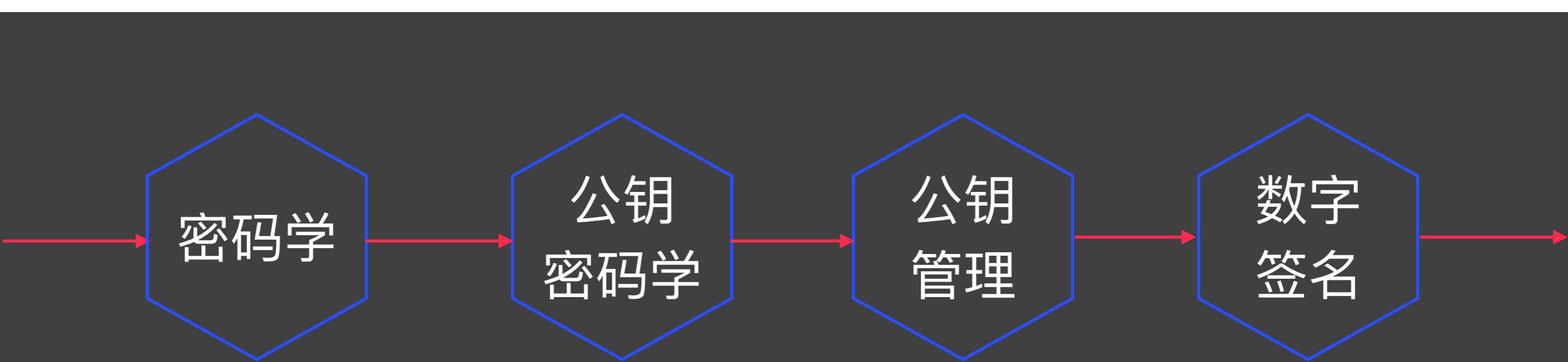
Number of Active Addresses on the Bitcoin Network (7DMA)



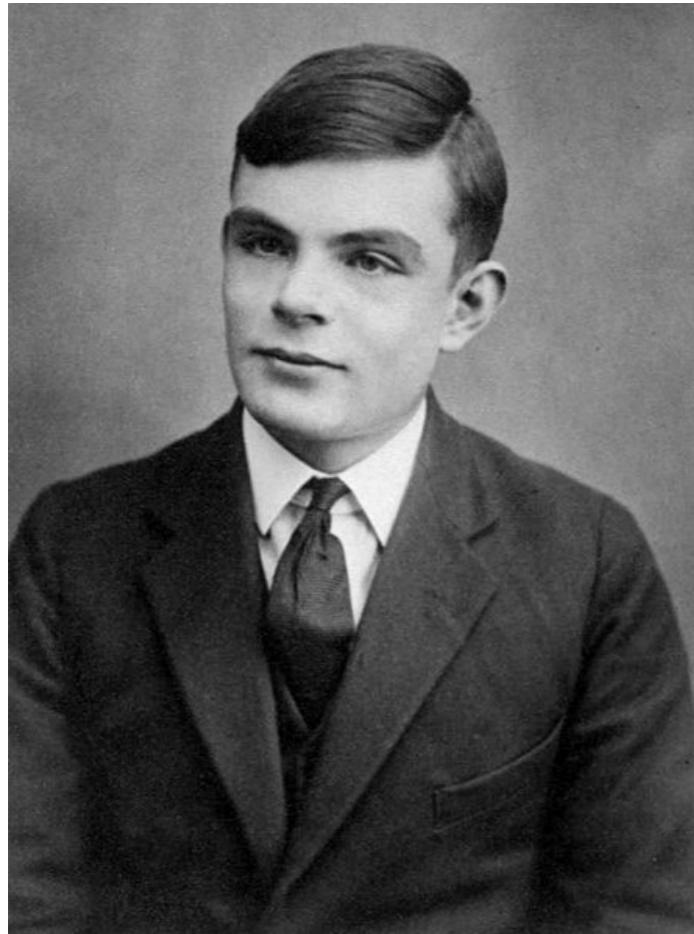
靓号地址

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

密码



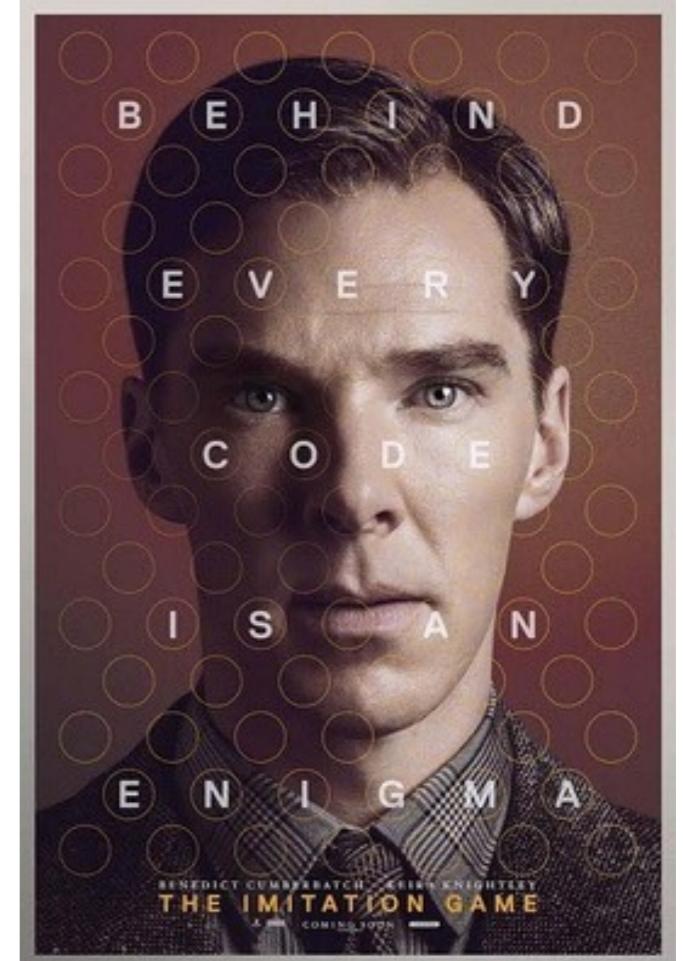
图灵



恩尼格玛密码机



模仿游戏



Hello World!

Encryption

\$\$\$\$&ZTF(
YSEW\$%TF
%&/(&RF/&%

Original Data

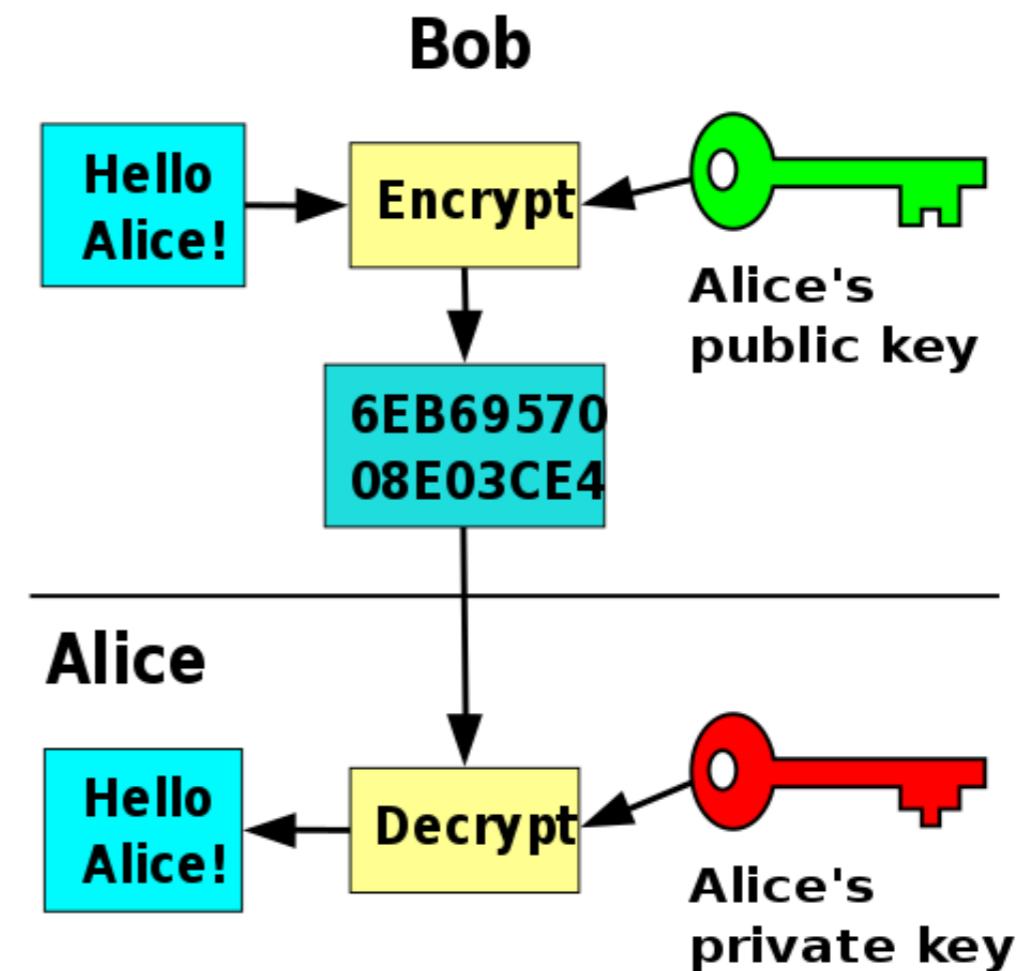
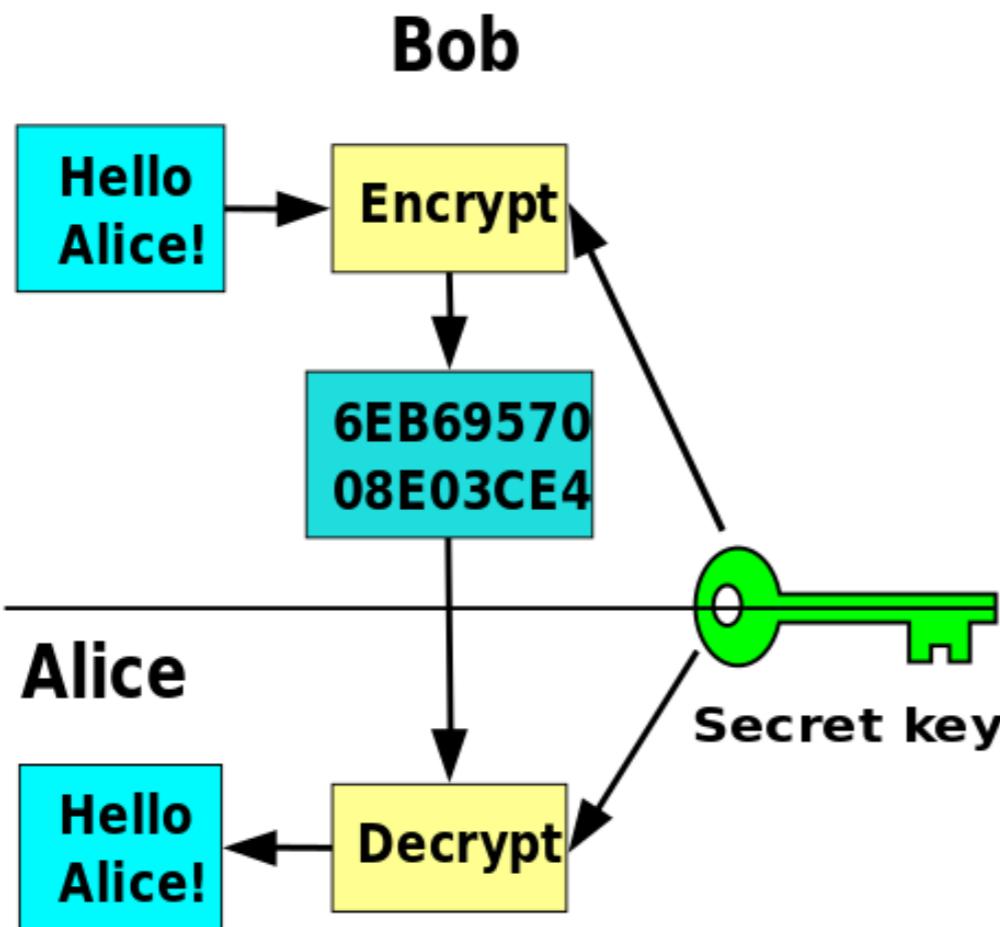
Decryption

Hello World!

Cypher Text

Original Data

对称密码学 vs. 非对称密码学



对称密码学

非对称密码学

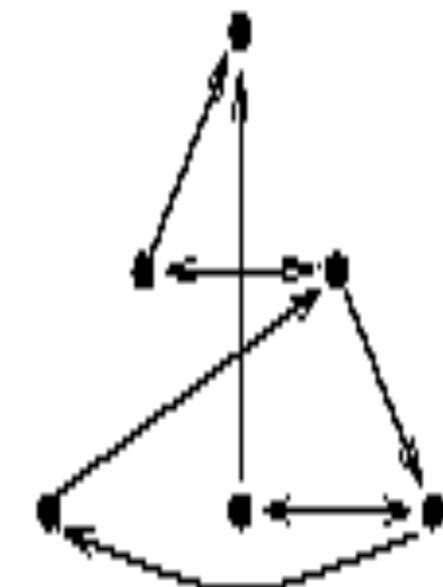
封闭

开放

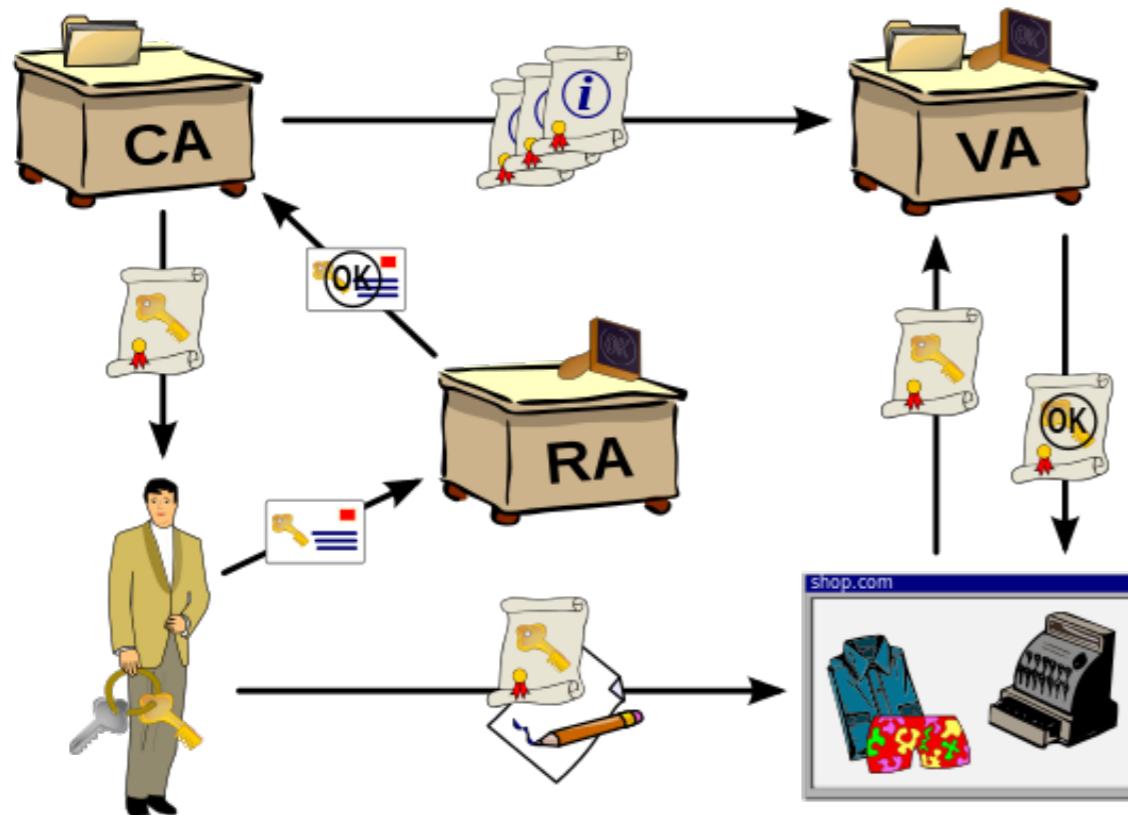
RSA



VERISIGN™



公钥管理
的P2P版本



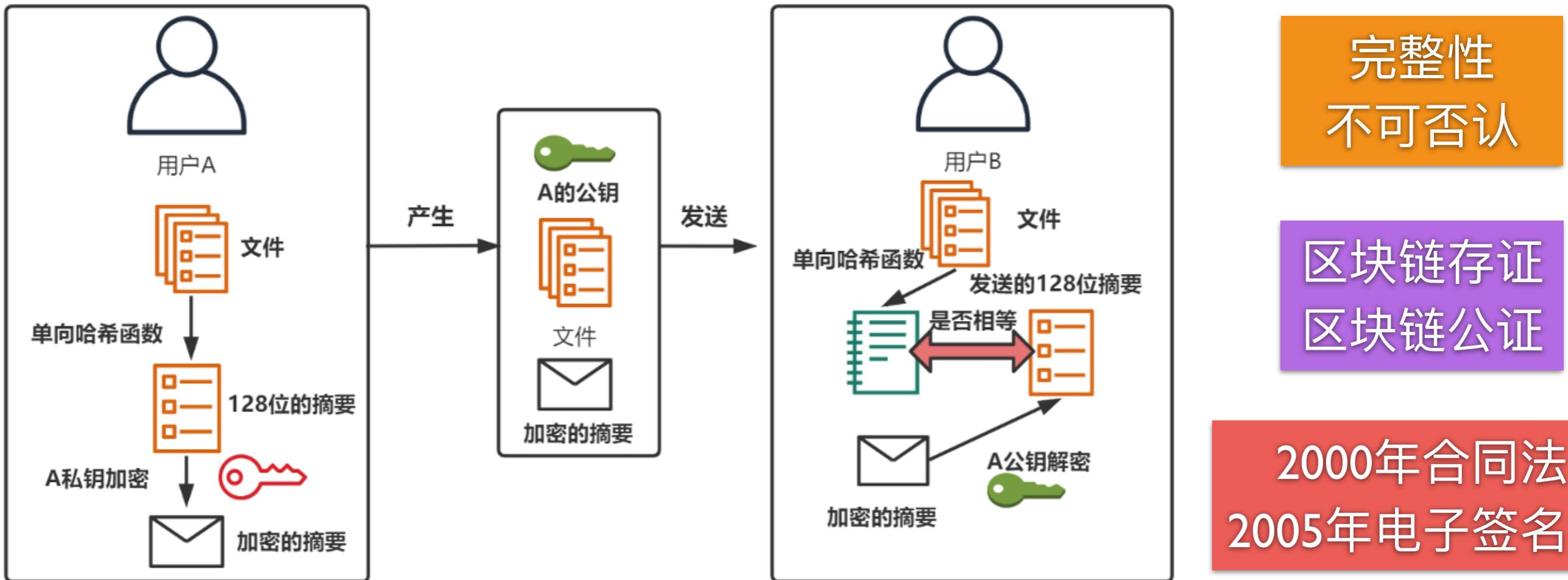
P G P®

1991

GnuPG
1999



Phil Zimmermann



1、文件经过单向散列函数的处理得到一份128位的摘要；

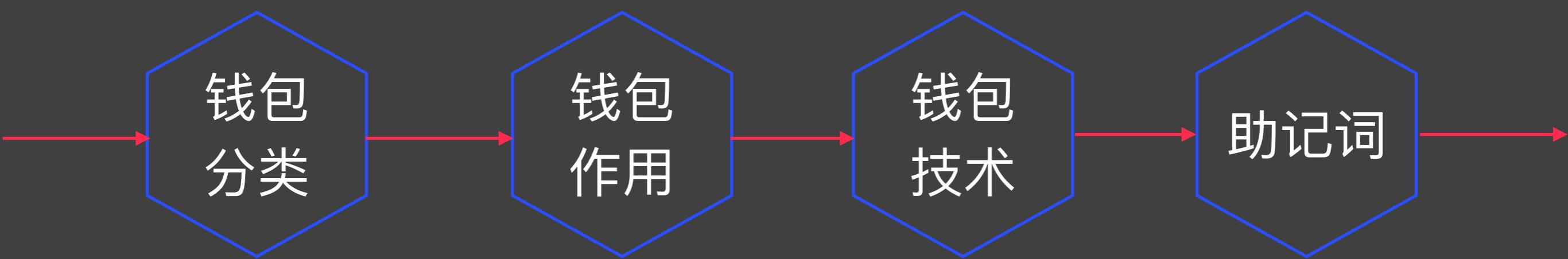
2、用户A使用自己地私钥对这份128位摘要进行加密，得到一份加密的摘要

3、用户A把文件、加密的摘要和公钥打包一起发给用户B

4、用户B将收到的文件经过单向散列函数处理得出一份128位摘要

5、如果两份摘要相等，说明文件经过用户A签名之后，在传输的过程中没有被更改；若不相等，说明文件在传输过程中被更改了，或者说不是原来的文件了，用户A的签名失效

钱包



Bitcoin

钱包分类

硬件钱包



安全硬件的一种应用。是一种为存储和管理比特币地址和私钥而设计的硬件，通过专门的硬件来存储私钥信息。

特点：硬件钱包的安全性较高，与网络隔绝，并在硬件本身层面也设置保护。不过硬件钱包往往价格较高，而且易用性有限。

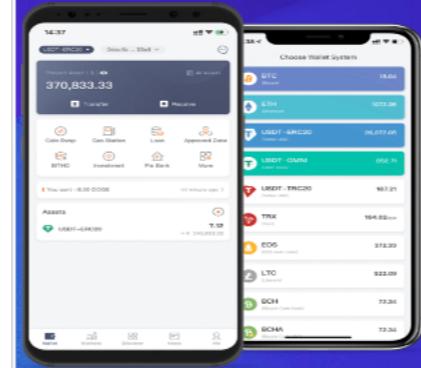
纸钱包



纸钱包也是一种离线冷钱包，其思路本质上就是“把私钥写在纸上”。

特点：纸钱包的离线性质使得其安全性较好。纸钱包一般也用作对硬件或其它存储介质的一种备份，存储于保险柜中。

手机钱包



手机钱包是以手机app形式进行密钥管理的钱包。

特点：其与移动结合的特性使得易用性较强，支持面对面使用QR码的快速交易。手机钱包一般由用户名密码登录，并在app内管理私钥。

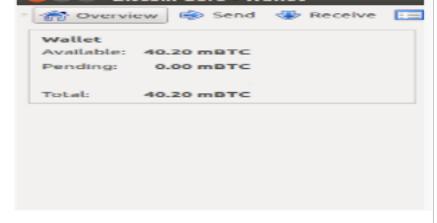
网络钱包



Web钱包将钱包实现为一种web服务。通过账号密码的方式在线访问和管理钱包，在服务器端备份密钥信息。

特点：因为它依赖于互联网，并且包含了对平台的信任。对服务器的攻击可能导致私钥被盗。因此，一般认为web钱包的安全性相对更低。

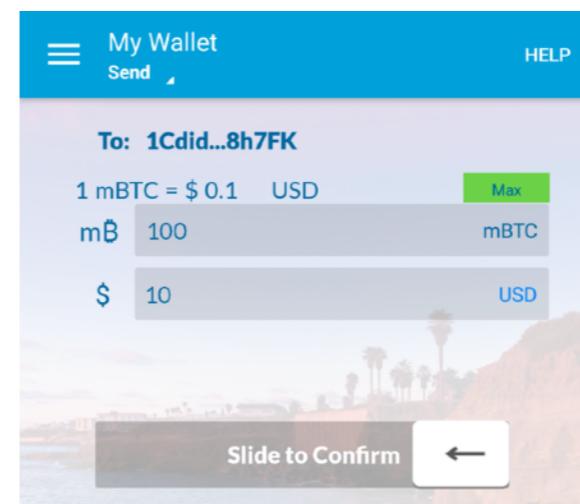
桌面钱包



桌面钱包将钱包实现为计算机桌面应用。桌面钱包的环境允许用户对自己的账户和资金有完整的掌握和控制，而不依赖在线服务商。

特点：一些桌面钱包的设计可以利用硬件支持，得到更高的安全性。并且桌面钱包软件一般还可以作为比特币全节点运行，参与挖矿过程等。

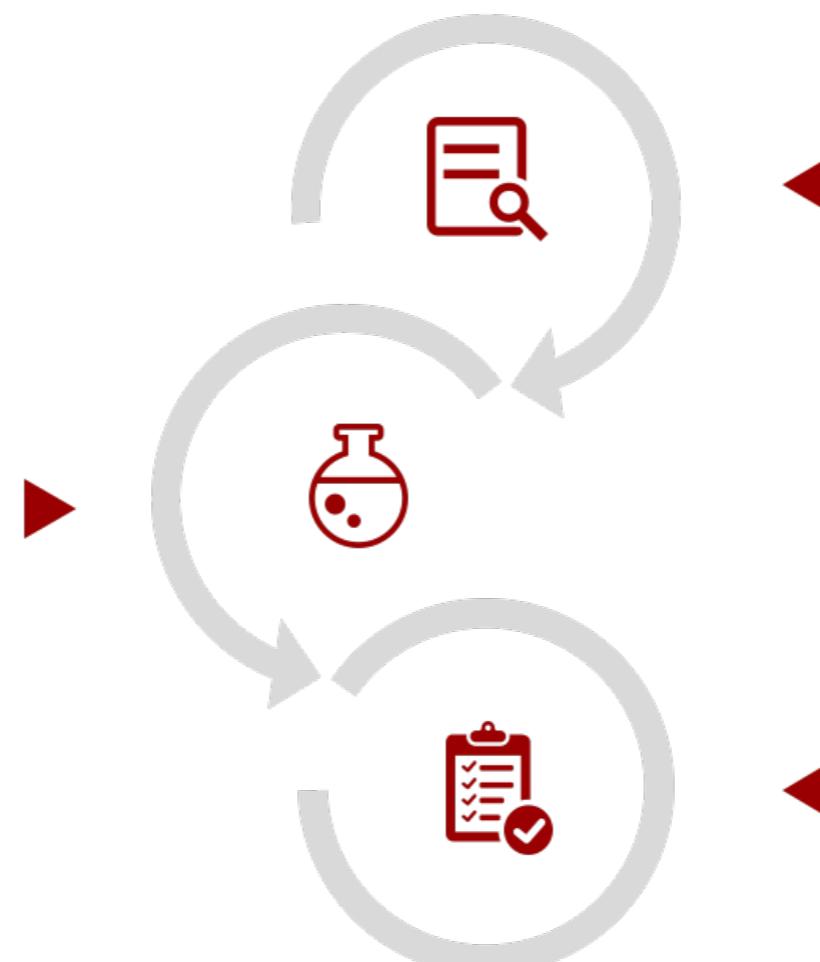
冷钱包指不接触互联网，不能通过网络访问的钱包，被通过网络攻击盗取风险更低，但是丢失风险更高，易用性相对较低。如果钱包损坏，恢复会十分困难，因此需要注意钱包备份。



热钱包一般是通过互联网管理的在线钱包，例如用户使用一个账户密码，通过平台管理自己的若干密钥。热钱包使用更方便，但安全性较低。

钱包作用

生成地址
使用用户的私钥生成公钥，并且使用公钥生成用户的地址，利用这些地址来接收其它用户给钱包的比特币转账。



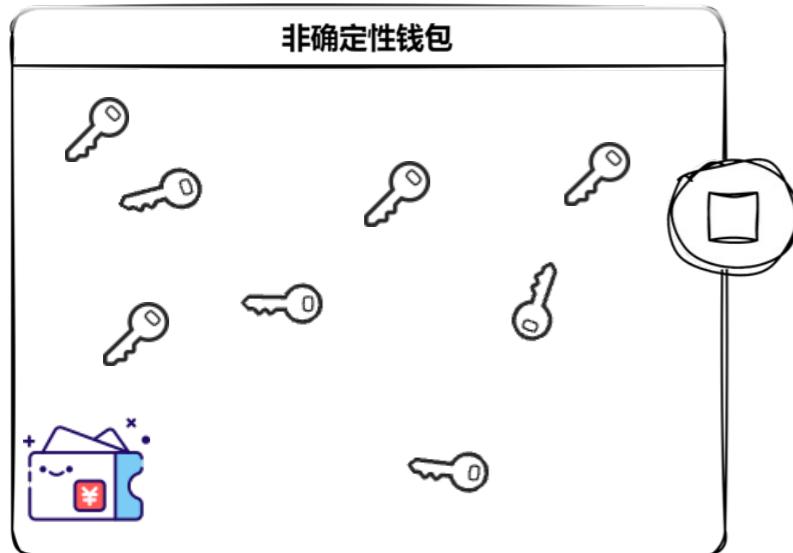
存储公私钥

存储和保管用户的私钥，并且使用用户的私钥对交易记录进行签名，以确保交易记录的安全性和不可否认性。

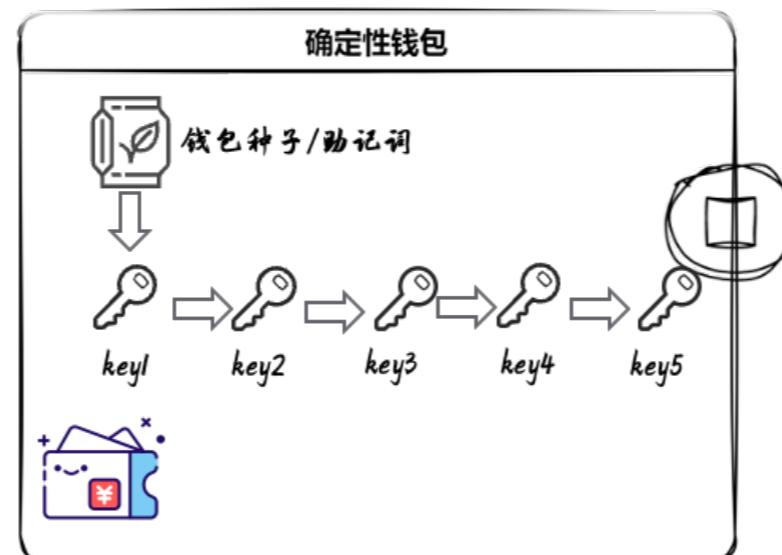
网络广播

将签名后的交易记录通过点对点网络广播给节点。

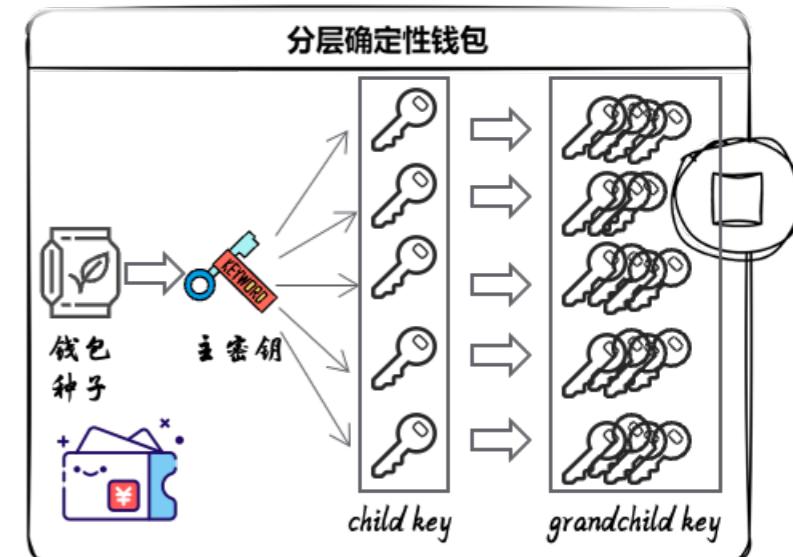
钱包技术



- 1、早期的比特币钱包模式，设计简单，难以备份，管理和导入
- 2、私钥是由没有逻辑关系的随机序列生成，因此私钥之间没有逻辑关系
- 3、多个无关联私钥的每一个都需要进行备份，产生了较大的管理开销



- 1、为了避免非确定性钱包备份开销问题，通过引入钱包种子（助记词）的方式，生成新的私钥序列。
- 2、只需要备份种子就可以保证恢复所有密钥，备份开销更小，恢复也十分便捷。



- 1、分层确定性钱包以树状的方式生成新的私钥。在备份和恢复的时候仍然只需要保存种子
- 2、具有主公钥属性，不仅可以用主公钥（种子直接生成）生成之后的所有私钥序列，还可以用对应的主公钥生成之后钱包中所有地址序列，并保证地址和生成的私钥对应。

随机钱包

种子钱包

HD钱包

JBOK
Just a Bunch of Keys

种子
一串随机生成的数字

BIP-32
BIP-39

BIP-43
BIP-44

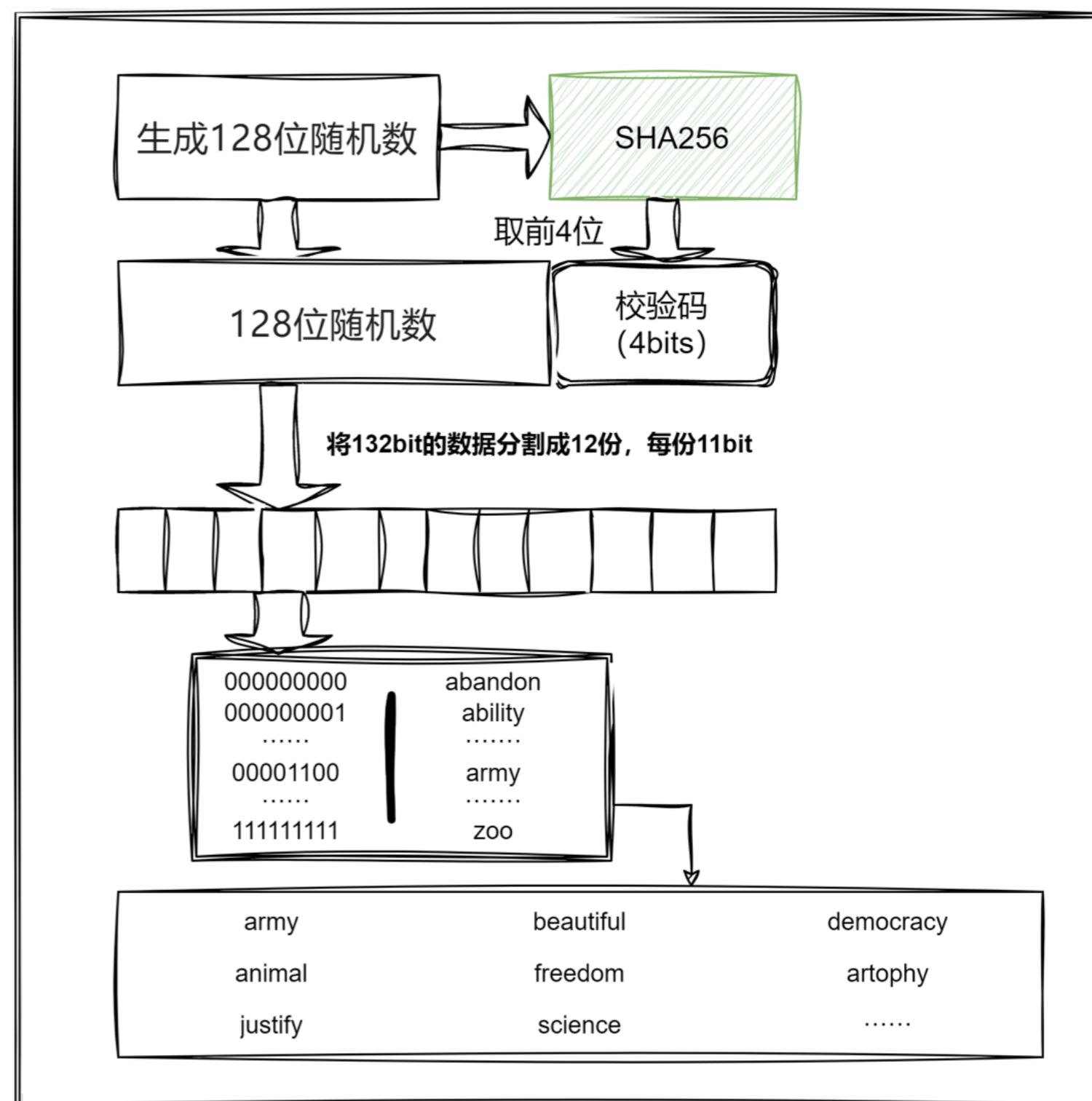
产生助记词

私钥

0fdc0ad9a0ea09e839767d6e8d90fedbf8f32d7aebd349893695daa4f51599e

64位随机数

- 1、生成128位随机数（BIP29中称为熵、Entropy、ENT）
 - 2、对随机数做SHA256，取前4位为验证码
 - 3、将1、2步骤中得到的结果拼接成一个132位的字符
 - 4、将132位的数按顺序平均分成12份，每份11个字符
 - 5、将11位字符转化为十进制数字，并查询BIP39中单词表，按顺序找到对应的单词
 - 6、这些查到的单词串就是一份助记



从助记词产生种子

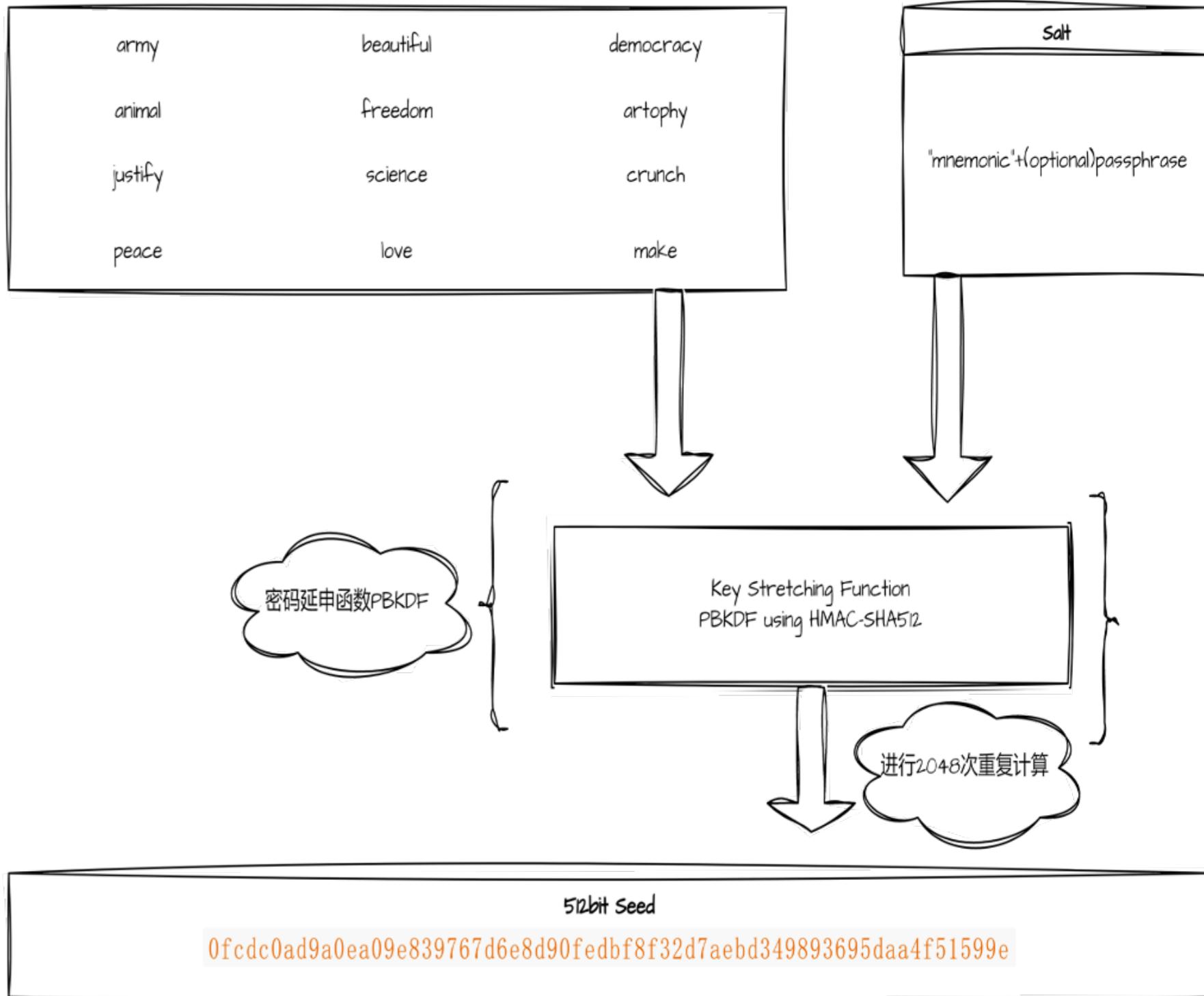
1、助记词作为密码
(Password)

2、HMAC-SHA512 作为
PBKDF2的随机函数 (HMAC)

3、进行2048次重复计算

4、将132位的数按顺序平均分
成12份，每份11个字符

5、生成一个512位 (64字节)
的种子 (dkLen)
种子 $DK = PBKDF2(HMAC, Password, Salt, c, dkLen)$



PBKDF2 Password-Based Key Derivation Function 2 是常用的拉伸函数算法中的一种

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 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

5b56c417303faa3fcba7e57400e120a0ca83ec5a4fc9ffba757fbe63fb77a89a1a3be4c6719
6f57c39a88b76373733891bfaba16ed27a813ceed498804c0570

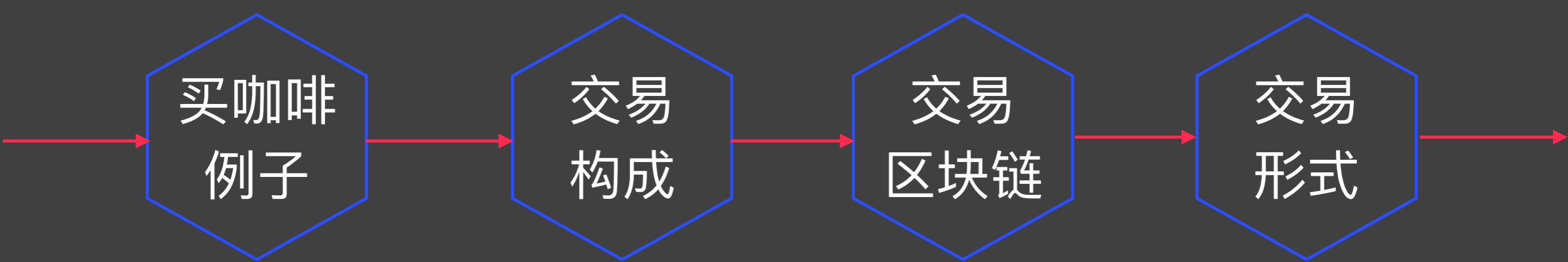
Coin

Bitcoin

BIP32 Root
Key

xprv9s21ZrQH143K3t4UZrNgeA3w861fwjYLaGwmPtQyPMmzshV2owVpfBSd2Q7YsHZ9j6
i6ddYjb5PLtUdMZn8LhvuCVhGcQntq5rn7JVMqnie

交易



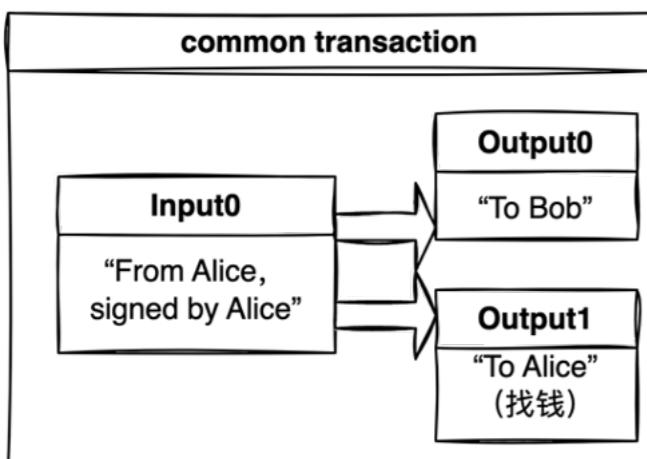
交易例子 - 买咖啡

```
bitcoin:1GdK9UzpHBzqzX2A9JFP3Di4weBwqqmoQA?  
amount=0.015&  
label=Bob%27s%20Cafe&  
message=Purchase%20at%20Bob%27s%20Cafe
```

A bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqqmoQA"
The payment amount: "0.015"
A label for the recipient address: "Bob's Cafe"
A description for the payment: "Purchase at Bob's Cafe"

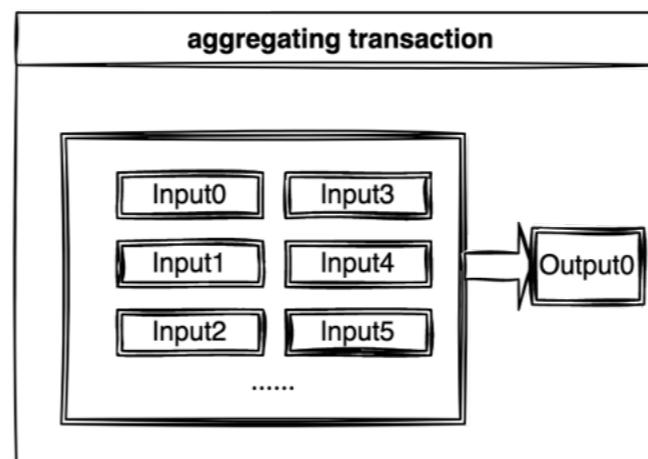
交易构成

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
$ \begin{array}{r} \text{Inputs} & 0.55 \text{ BTC} \\ - \text{Outputs} & 0.50 \text{ BTC} \\ \hline \text{Difference} & 0.05 \text{ BTC} \text{ (implied transaction fee)} \end{array} $			

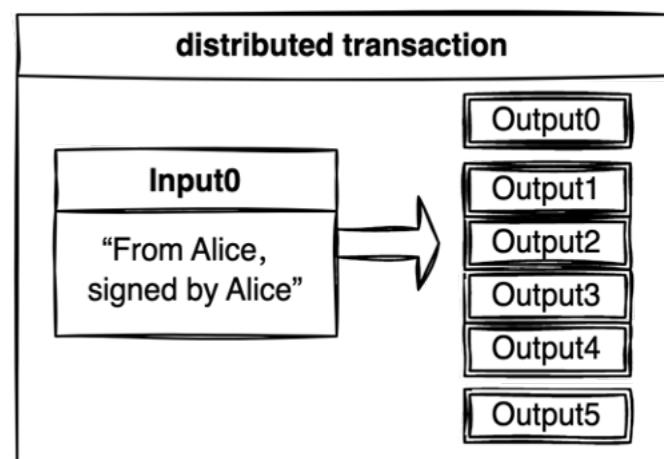


找零

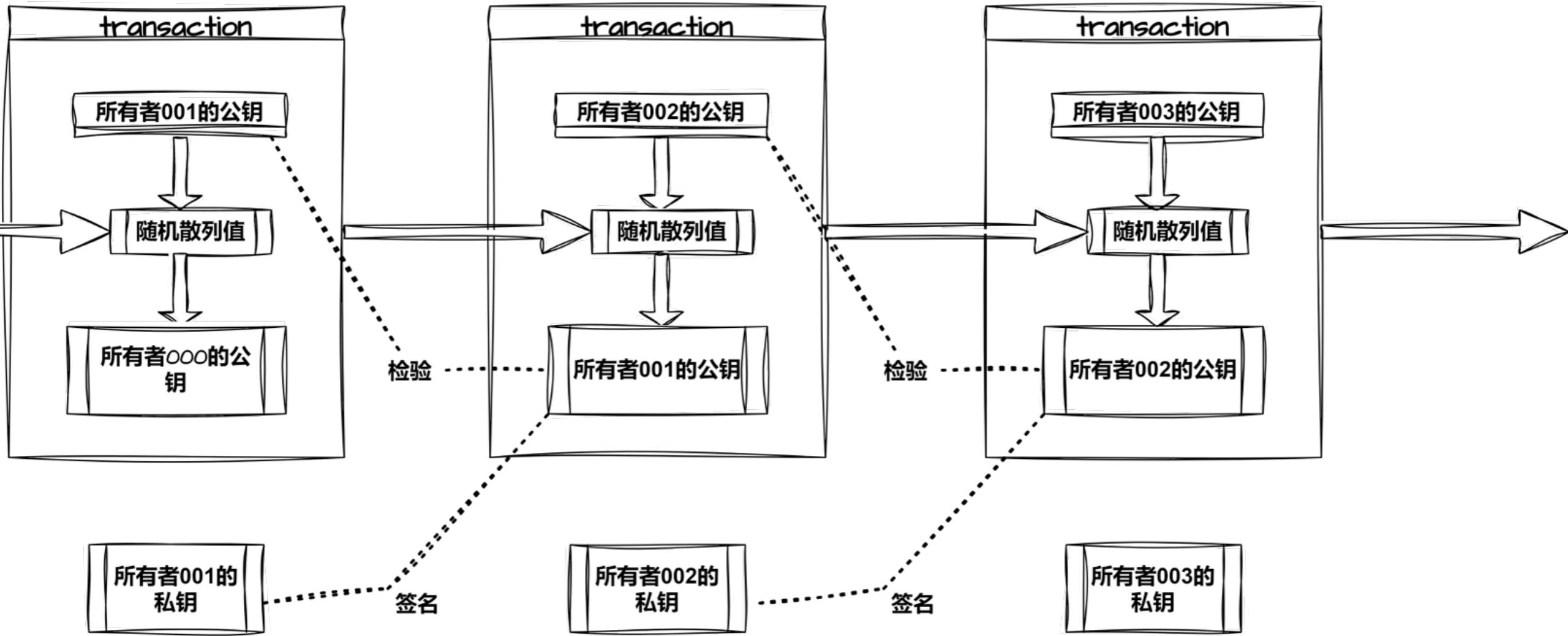
归集



分发



交易链描述



比特币中，存储的只有交易信息使用**收款人的公钥**对交易内容进行加密，这样就只有收款人才能解密

消息中包发送者的公钥，使用**发送者的私钥**进行签名，这样就能确认该交易是属于发送者的，并且该消息确实是发送者所发送的

区块链浏览器

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

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**

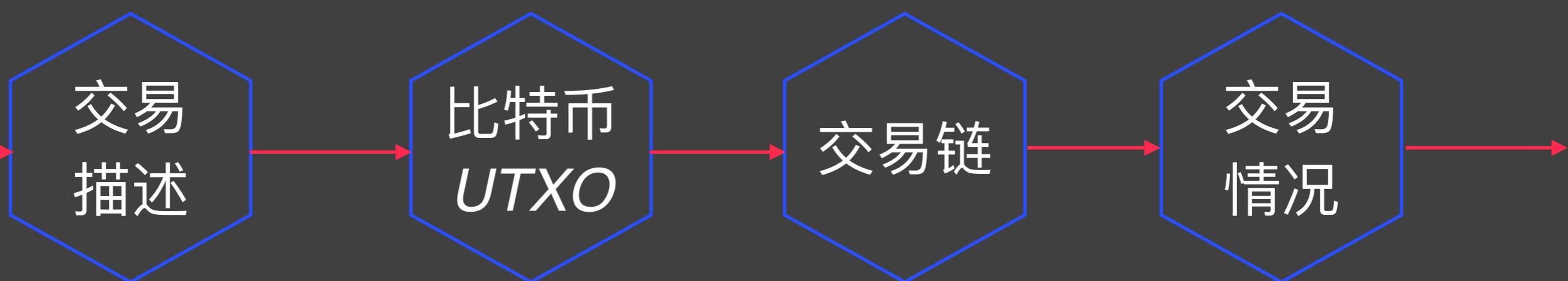
Total Input 0.1 BTC

Total Output 0.0995 BTC

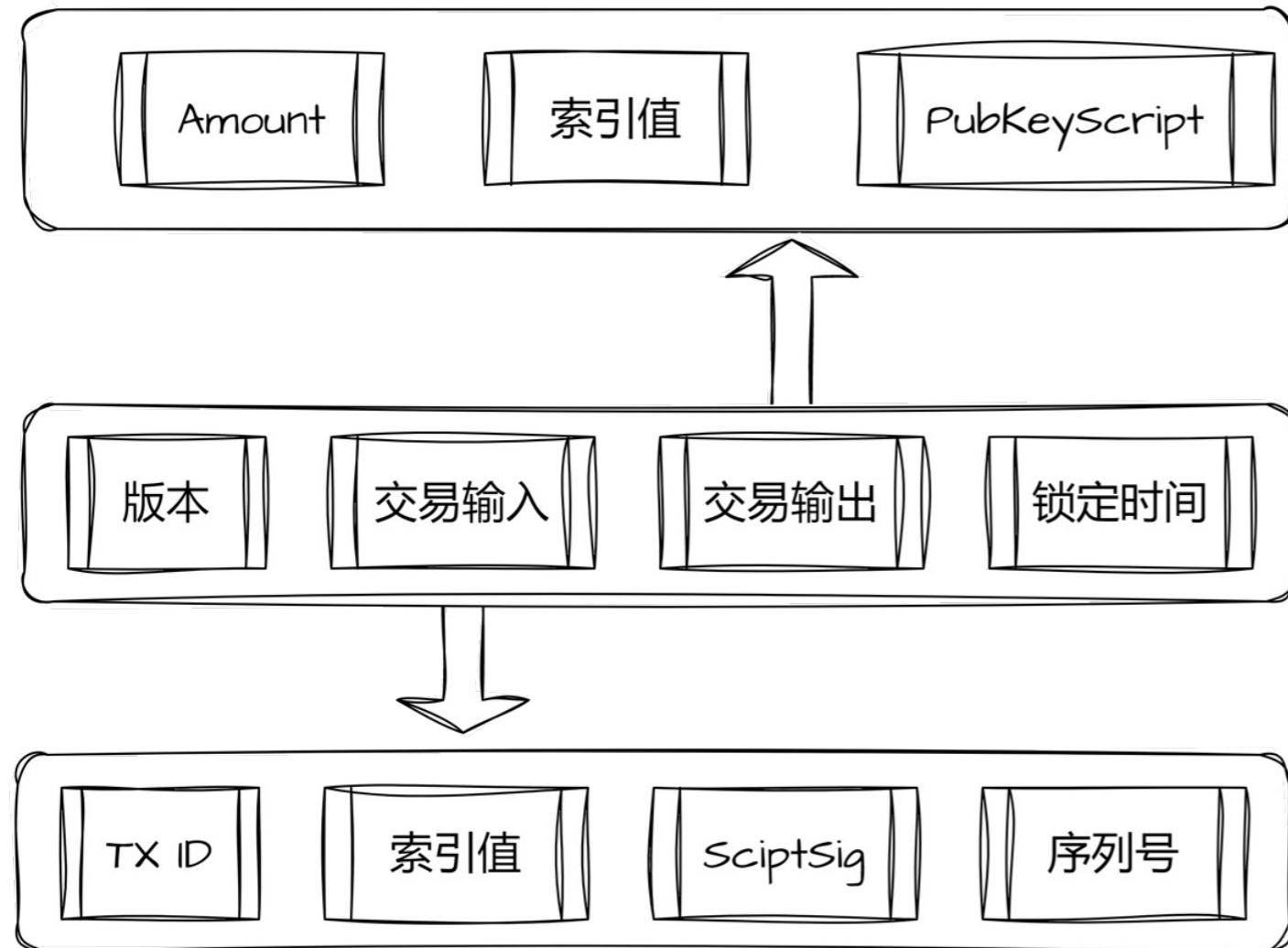
Fees 0.0005 BTC

Estimated BTC Transacted 0.015 BTC

UTXO



交易描述

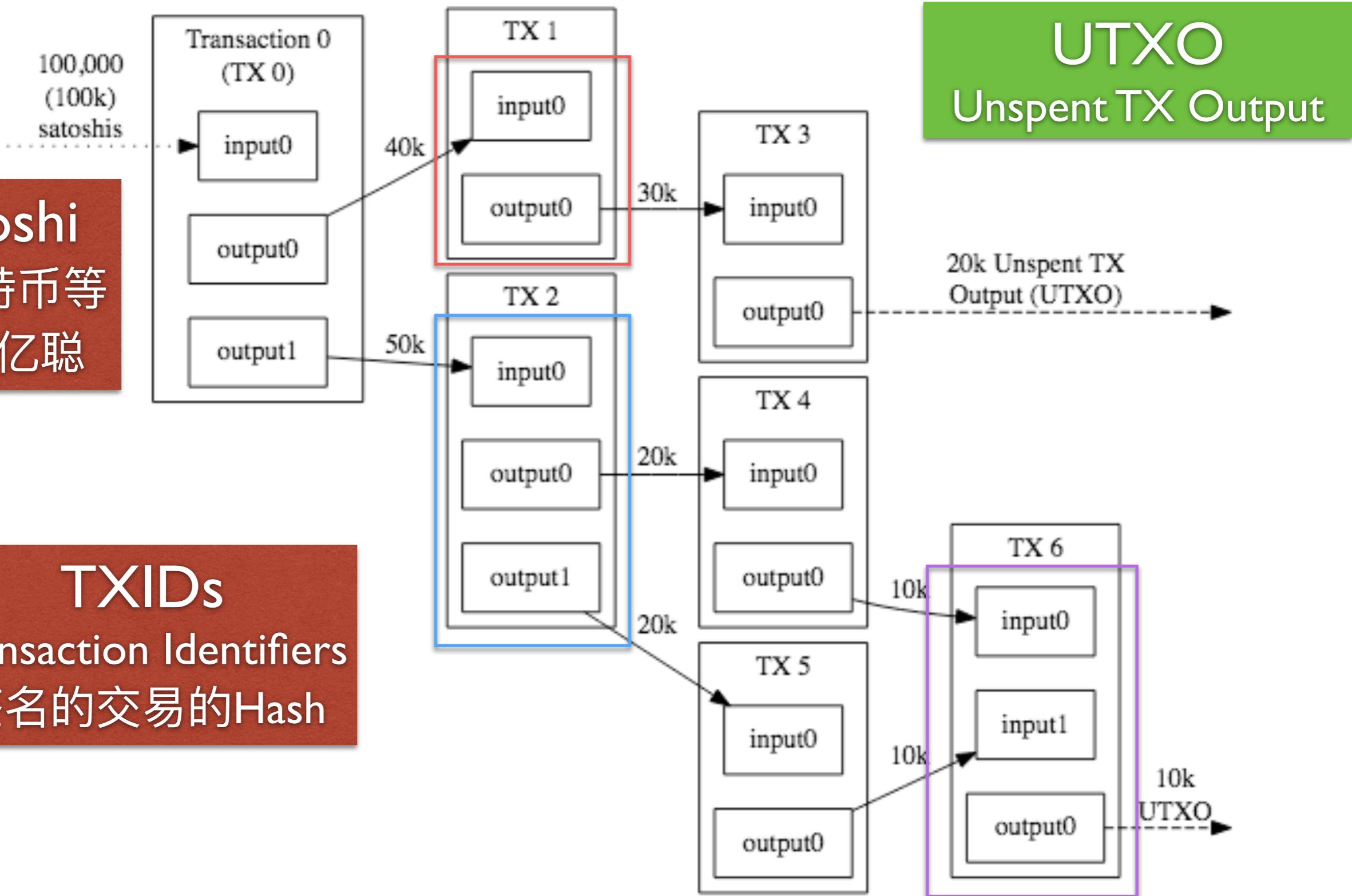


如图所示，比特币交易的主要构成部分，包括版本信息、交易输入、交易输出和锁定时间。

每一笔比特币交易中具有一个四字节的交易版本号，它告知比特币节点和矿工应该使用哪一套规则用来验证这笔交易，使得开发者在为未来的交易创建新的规则时可以不验证之前产生的交易；

每一笔交易中至少包含一个交易输入和一个交易输出，每个交易输入会花费上一个交易输出产生的比特币，每个交易输出都作为UTXO直到被作为交易输入花费掉。

比特币UTXO



交易链

Transaction 7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18

INPUTS From		OUTPUTS To	
From (previous transactions Joe has received):		Output #0 Alice's Address	0.1000 BTC (spent)
Joe	0.1005 BTC	Transaction Fees:	0.0005 BTC

Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2

INPUTS From		OUTPUTS To	
7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18:0		Output #0 Bob's Address	0.0150 BTC (spent)
Alice	0.1000 BTC	Output #1 Alice's Address (change)	0.0845 BTC (unspent)
		Transaction Fees:	0.0005 BTC

Transaction 2bbac8bb3a57a2363407ac8c16a67015ed2e88a4388af58cf90299e0744d3de4

INPUTS From		OUTPUTS To	
0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fb8a57286c345c2f2:0		Output #0 Gopesh's Address	0.0100 BTC (unspent)
Bob	0.0150 BTC	Output #1 Bob's Address (change)	0.0045 BTC (unspent)
		Transaction Fees:	0.0005 BTC



Transactions on the Bitcoin Network (Daily, 7DMA)



450k

400k

350k

300k

250k

200k

150k

Jul '17

Jan '18

Jul '18

Jan '19

Jul '19

Jan '20

Jul '20

Jan '21

Jul '21

Jan '22

Jul '22

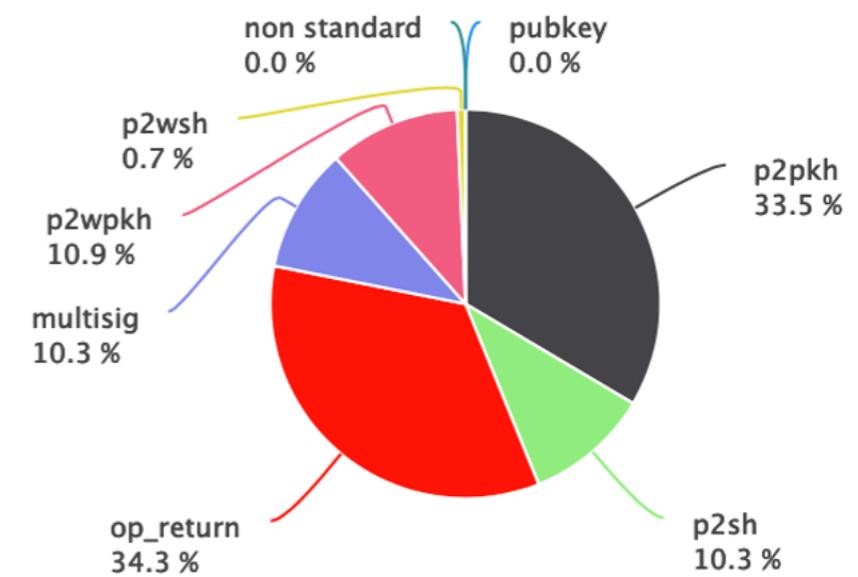
SOURCE: COIN METRICS
UPDATED: NOV 5, 2022

ZOOM ALL YTD 12M 3M 1M

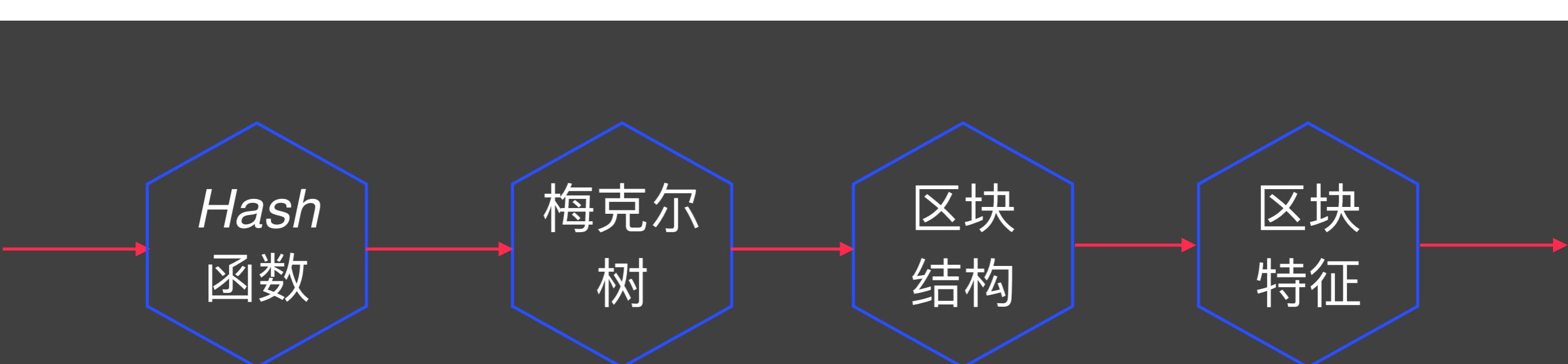
比特币网络每日交易数量变化

Transaction unspent outputs (UTXO)

PUBKEY	48 081
P2PKH	50 636 443
P2SH	15 598 968
MULTISIG	438 042
P2WPKH	16 395 243
P2WSH	1 007 057
NON STANDARD	9 149
OP_RETURN	51 768 629
OP_RETURN_NON_STANDARD	36 807
Total	136 121 606
Total spendable	84 316 170



区块



Hash函数

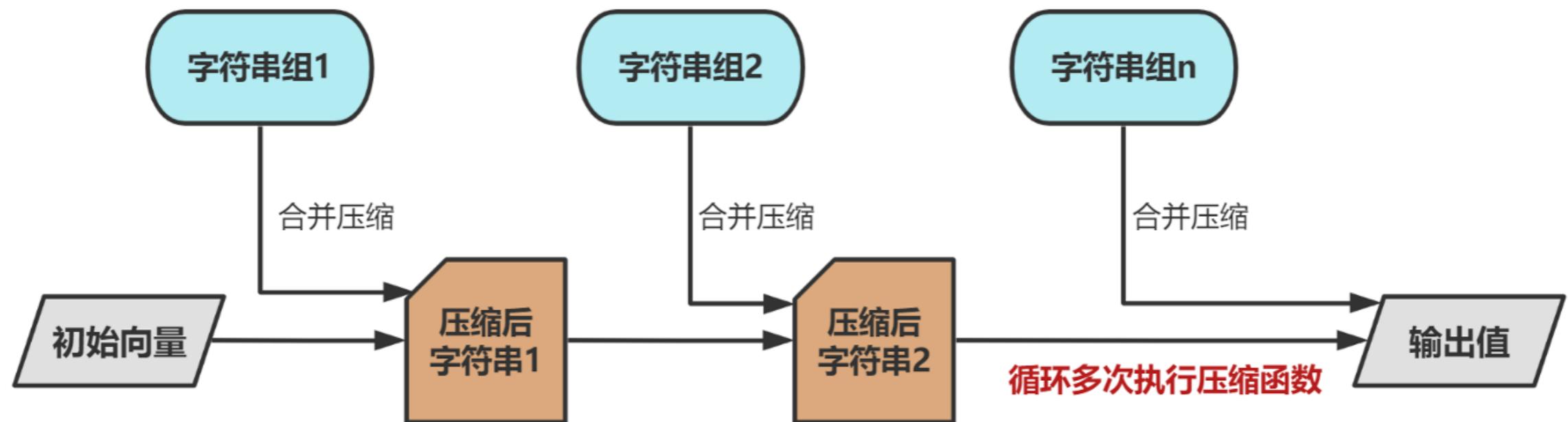
https://en.wikipedia.org/wiki/Hash_function

输入为任意大小的字符串

可以进行有效计算：例如 $O(n)$

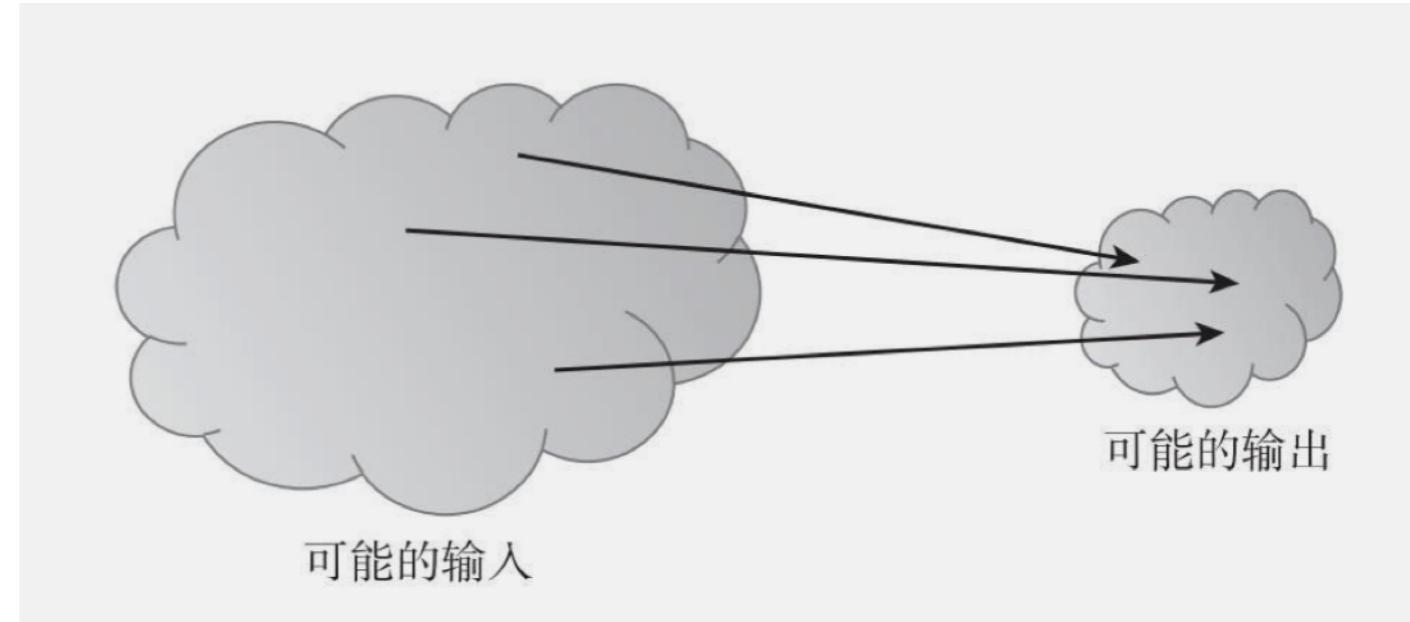
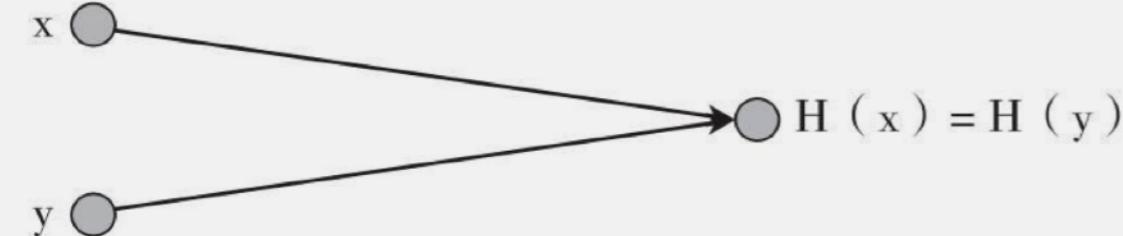
输出为固定大小，例如256位

同样的输入产生同样的输出

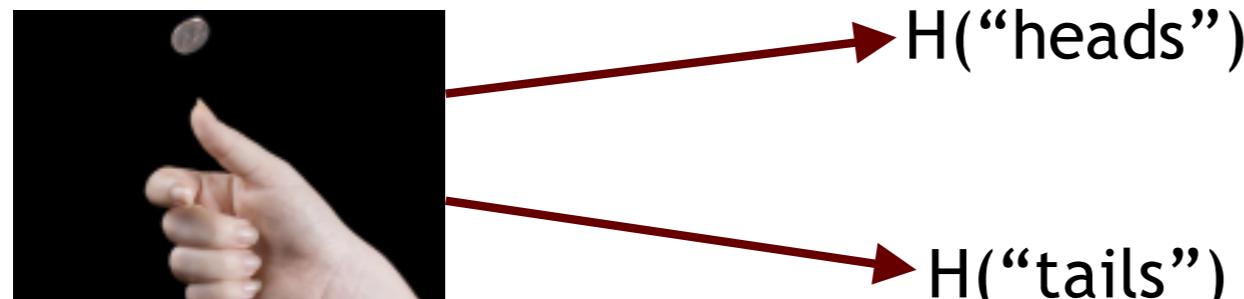


Hash函数

抗碰撞



隐匿性



给出 $H(x)$, 不能找到 x

单向性

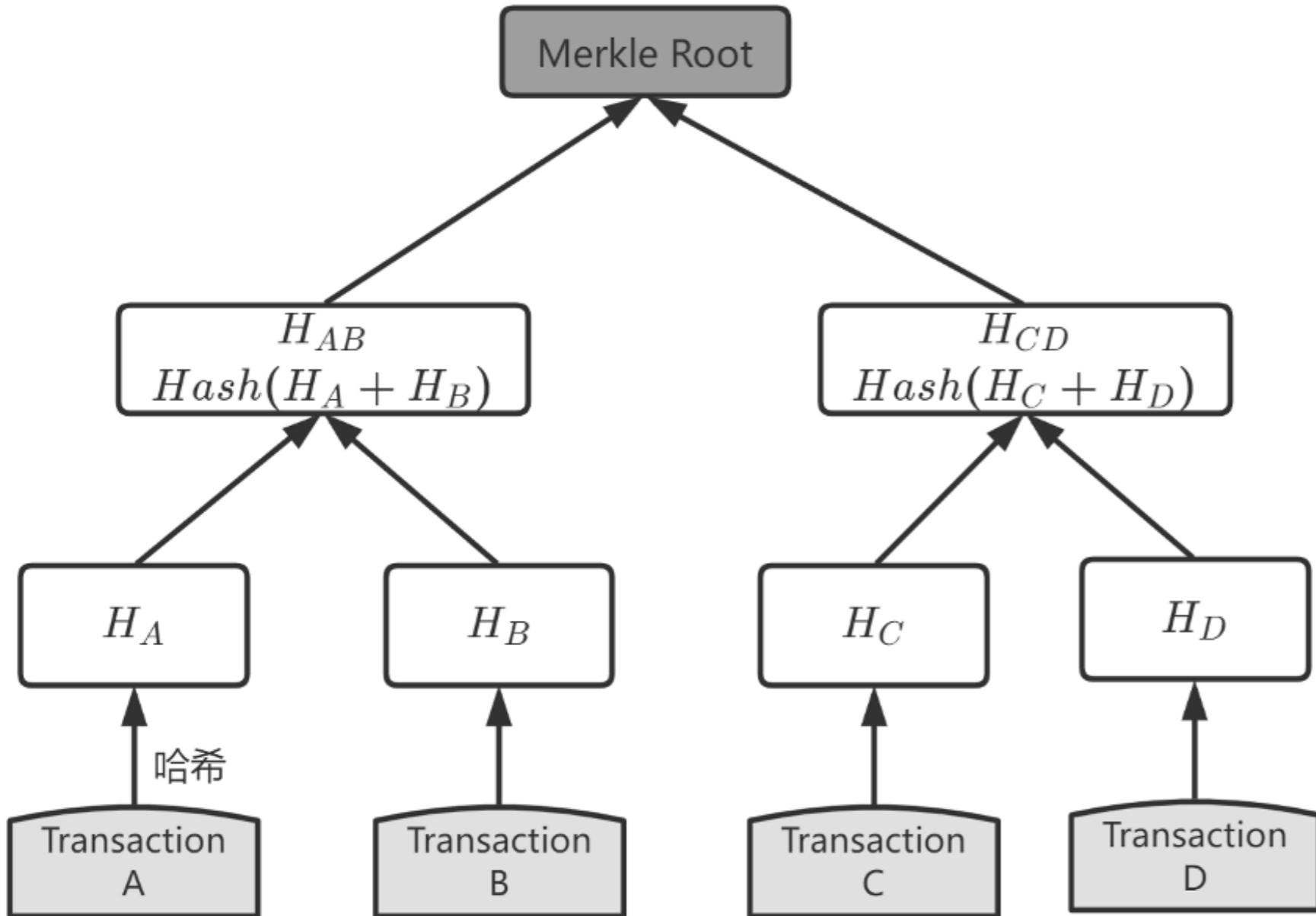
已知 x , 计算 $H(x)$ 容易

已知 $H(x)$, 求 x 困难

难题友好

梅克尔树

梅克尔树是使用Hash指针替代了二叉树的普通指针，最初的设计目的是为了提供数据的存证，叶子结点是具体的交易、梅克尔树不仅可以检查数据的存在性，如果是排序的梅克尔树，还可以检查数据是否不存在于该树中

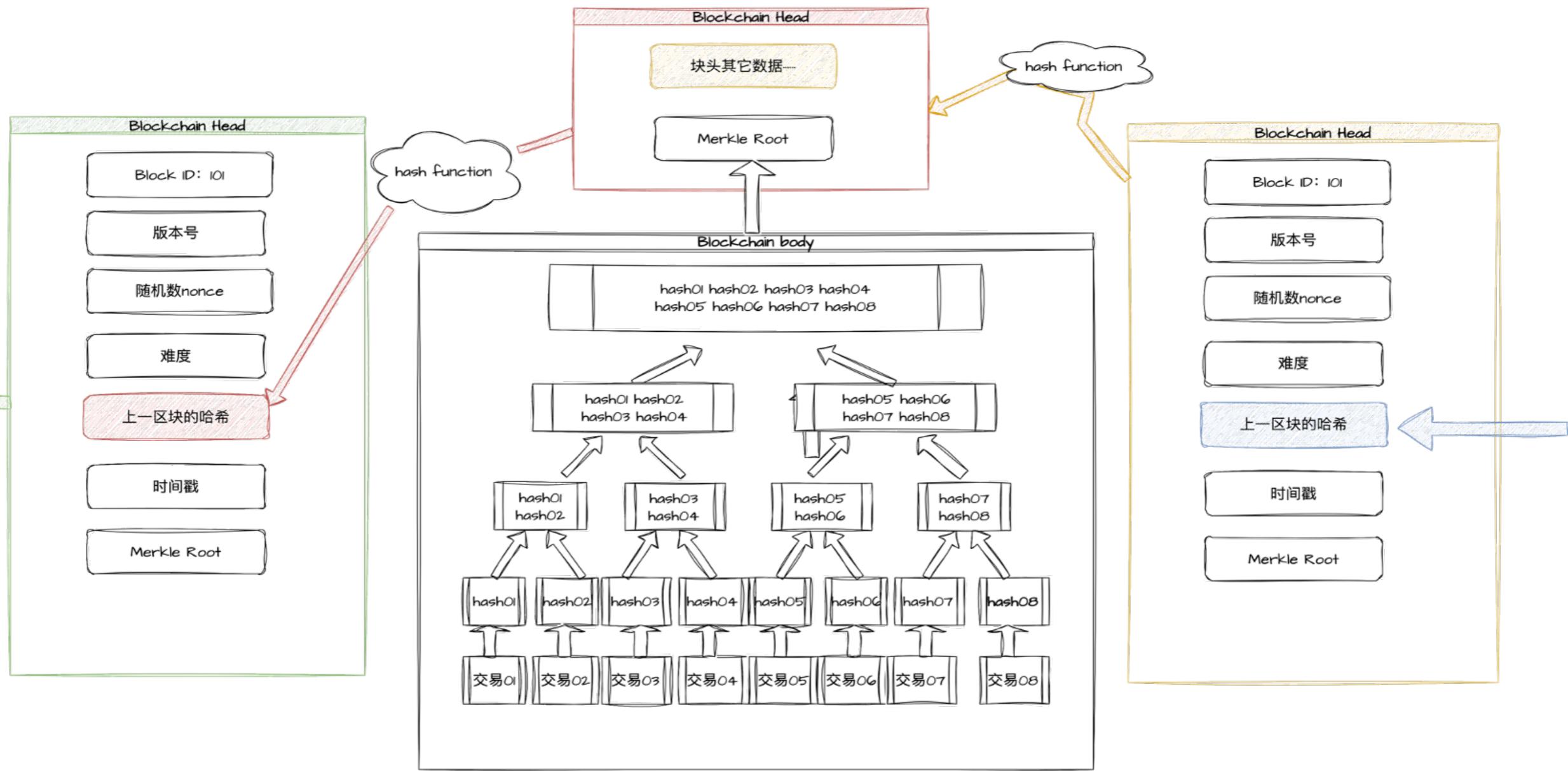


在单个区块中有成百上千的交易是非常普遍的，这些交易都会采用同样的方法归纳起来，产生一个仅仅32字节的数据作为梅克尔树根

为了证明区块中存在某个特定的交易，一个节点只需要计算 $\log_2(N)$ 个32字节的哈希值，形成一条从特定交易到树根的认证路径或者Merkle路径即可

随着交易数量的急剧增加，这样的计算量就显得异常重要，因为相对于交易数量的增长，以基底为2的交易数量的对数的增长会缓慢许多

区块结构



Bitcoin block 0  mined by  Anonymus

Time	2009-01-03 18:15:05	Coinbase message
Transactions	1	
Size	285 bytes	Block
Stripped size	285 bytes	Previous block
Weight	1 140	Next block
Block difficulty	2 536	Merkle root
Network difficulty	1	
Version	0x01	Coinbase hex
Bits	0x1d00ffff	<pre>04ffff001d0104 07365636f6e642</pre>
Nonce	0x7c2bac1d	
Block reward	50.00000000 BTC	Header
Fee reward	0 BTC	

The Times 03/Jan/2009 Chancellor on brink of second bailout for banks

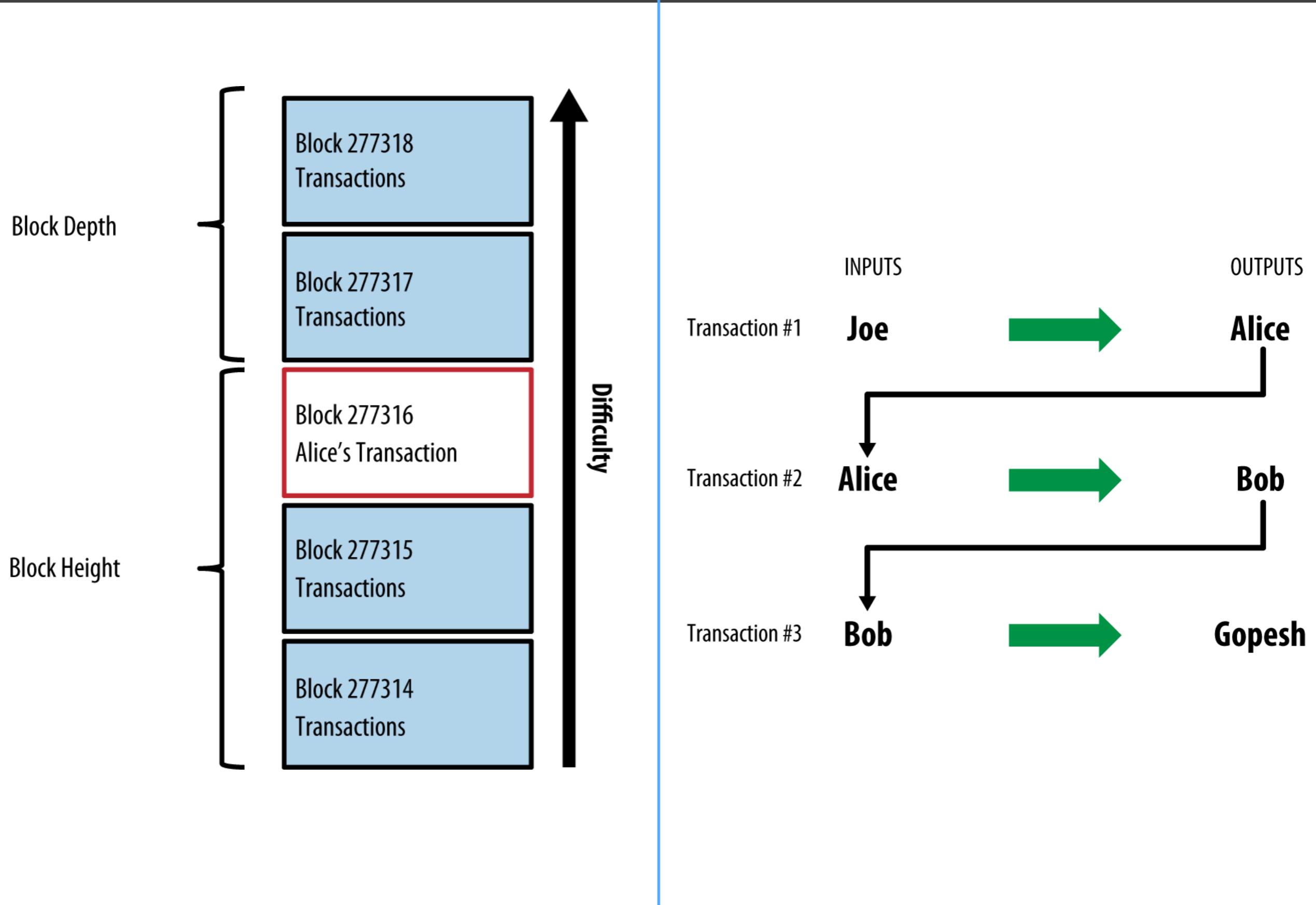
Coinbase hex

04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f662
07365636f6e64206261696c6f757420666f722062616e6b73

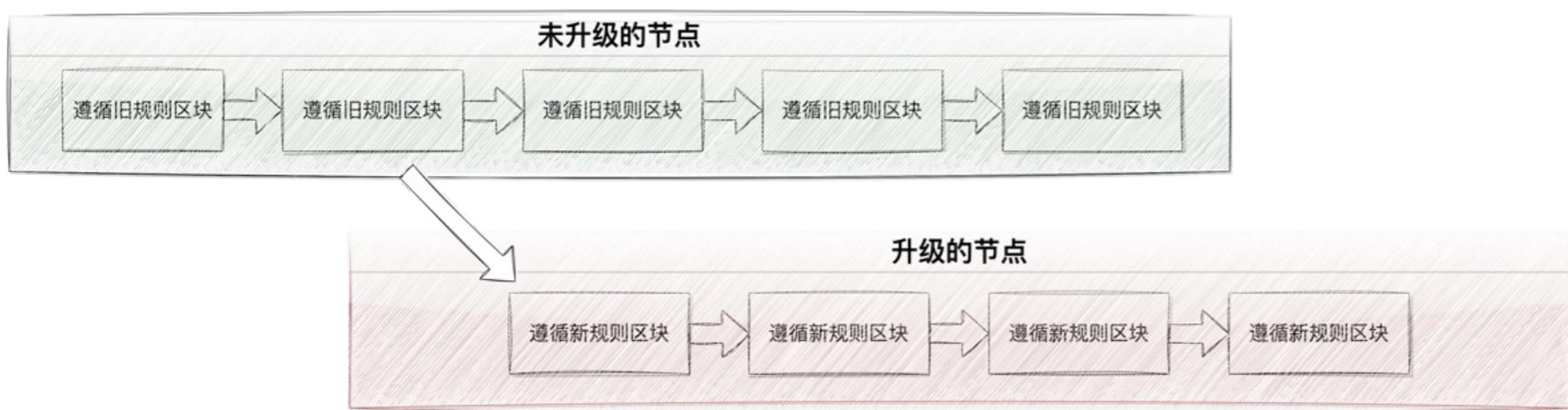
北京时间2009年1月4日（当地时间1月3日），一个名为“中本聪”的极客在位于芬兰赫尔辛基的一个小型服务器上，亲手创建了第一个区块，即比特币创世区块，并获得了第一笔50枚比特币的奖励。就在这一天，第一枚比特币诞生了。当时，中本聪将当天泰晤士报的头版“总理已经濒临对银行第二次救助的边缘”记录在了创世区块之中。这不但清晰地展示着比特币的诞生时间，还表达着对旧体系的嘲讽。



区块高度和深度

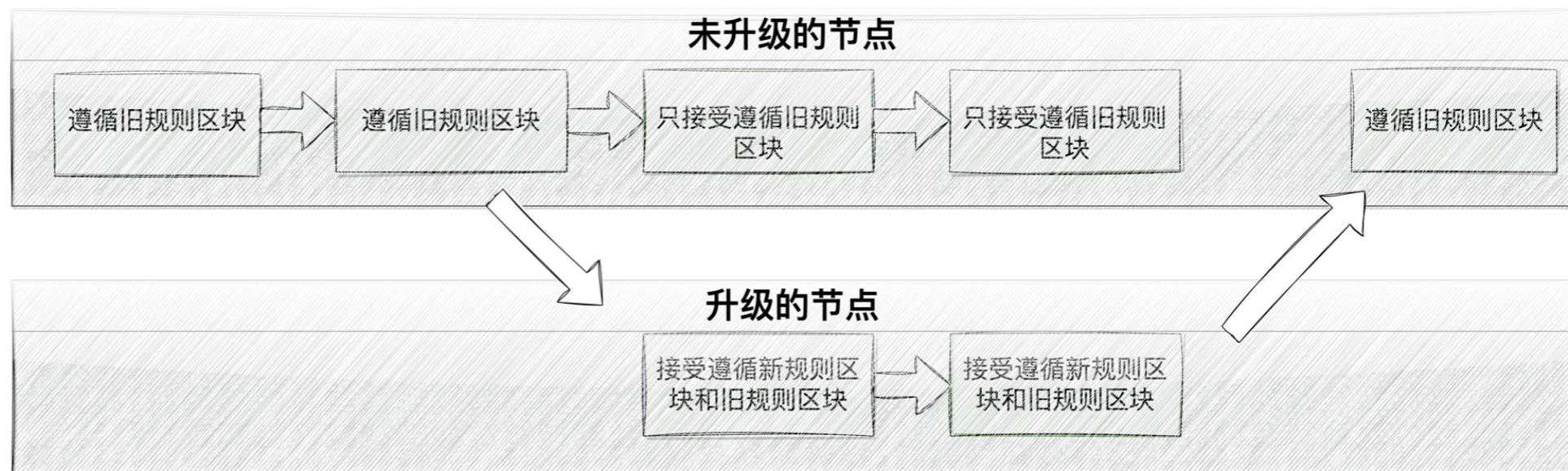


分叉

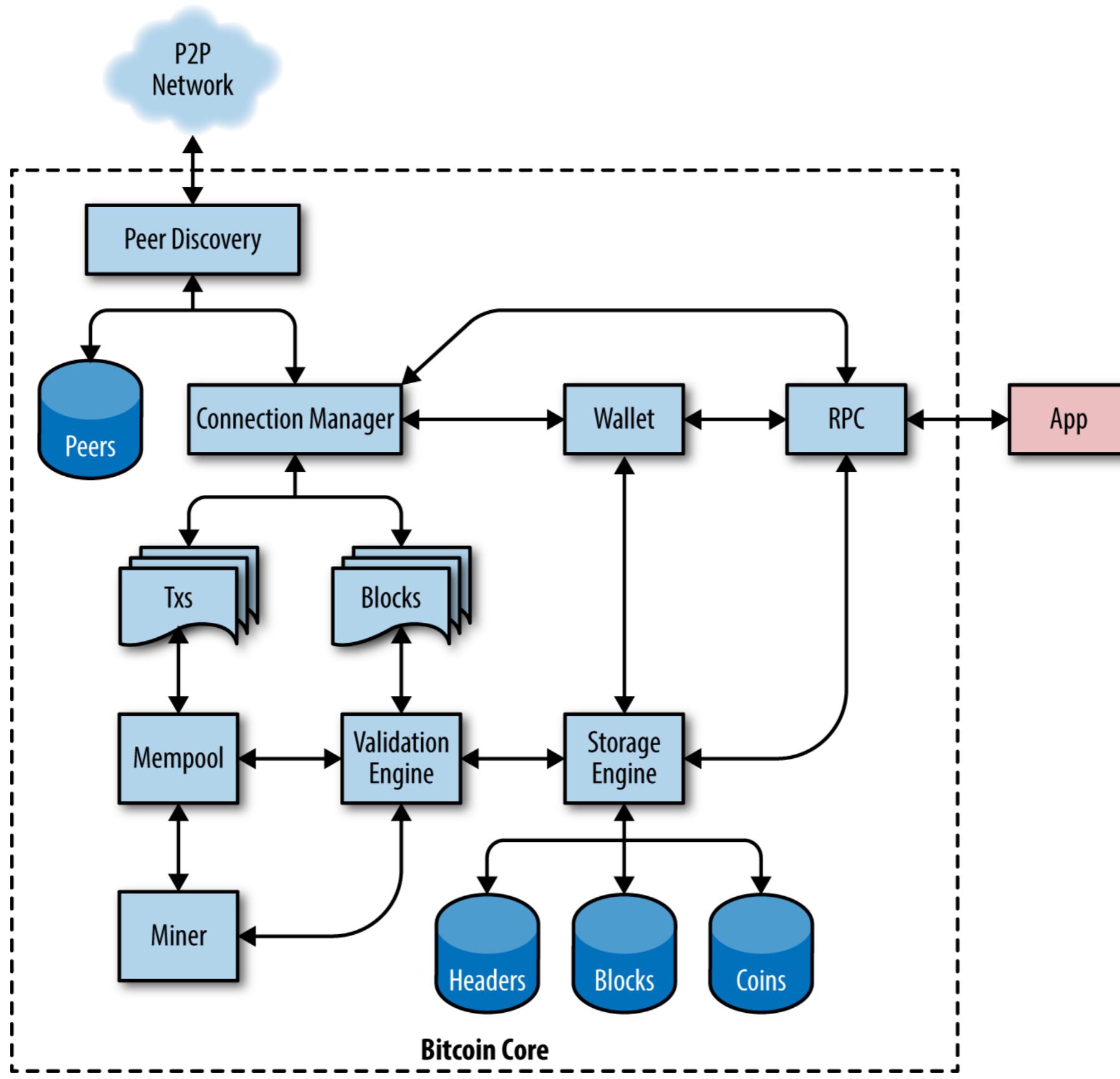


在硬分叉的情况下，因为那些未升级的节点会拒绝接受新规则的块，从而未升级节点产生的区块会在未升级节点构成的链上被接受。升级节点产生的块会在升级节点构成的链上被接受，从而产生了两个独立的链，产生了永久的分叉。

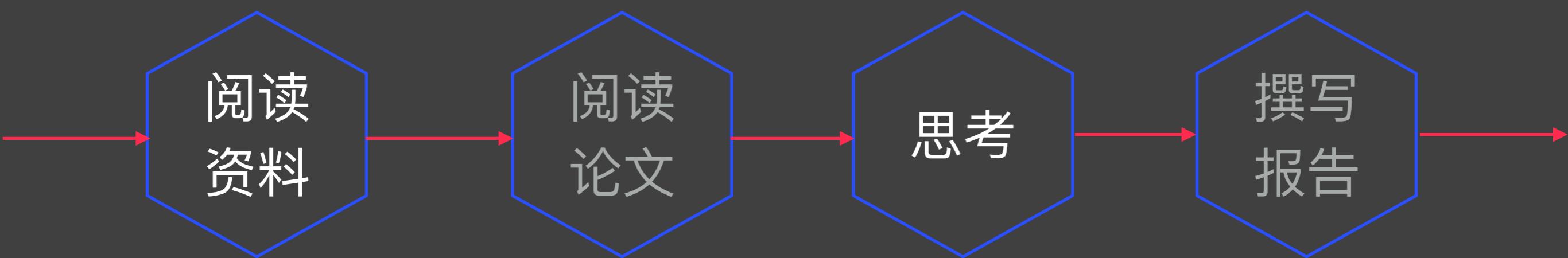
在软分叉的情况下，如果升级的节点掌握了大多数的算力，则可以防产生永久的分叉，因为这些升级的节点占有大多数算力，可以构造最长有效链，最终未升级的节点将接受其作为最长有效链。



Bitcoin核心架构



课后作业



Homework

课后阅读建议



第1、2、4、5、6、9章

<https://www.8btc.com/book/281955>

<https://github.com/bitcoinbook/bitcoinbook>

<https://www.bitcoin.org/>

介绍性内容
Introduction
White Paper

开发方面内容
Developer Guides、Reference、
Examples、Learning Resources

谢谢！

孙惠平

sunhp@ss.pku.edu.cn