BLOCKCHAIN

2010年5月，一位程序员用10000个比特币购买了这样的两个披萨

图片来自：https://en.bitcoin.it/wiki/Laszlo_Hanyecz

2017年12月，10000比特币大约值1.8亿美元

挖矿？

区块链？

区块链

一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构， 并以密码学方式保证的不可篡改和不可伪造的分布式账本。

不可篡改

链式结构

1.不可篡改性

Bob付50元给Alice

Bob付30元给Dan

?

Alice

Bob

Cindy

Dan

哈希算法

SHA-256
(Bob付20元给Dan)

=

10110110100101111011100110010000
10111001011110000100010111001100
10111101110001101100001111111110
11000110100101110010001111101110
10000111001111110010001110001110
00110110111101110110101100101001
11110011100101000101010011010000
00010001110101111001010100101111

哈希算法

SHA-256
(Bob付30元给Dan)

=

10000001010010110101000010110010
10111001001111011000011100010011
00011011001011101001000101101000
10001110000100010110101100000000
11010001111010011101100011101111
01100100010000000101001000010111
10001100110010010011100001010110
00001111111000100101001011111100

哈希算法

SHA-256
(Bob付30元给Dan!)

=

11000100111100010110001101000111
01111101100111010100010111010110
01110110110010010111010000110010
00110010011111010010001011011100
00110100110000111111101000110110
01100100011100000010000010110000
00011110011110101001110100110010
01010000110111111110010001000010

完全随机，无规律可循

Bob付50元给Alice

Bob付20元给Dan

Alice

Bob

Cindy

Dan

Bob付50BTC给Alice

Bob付20BTC给Dan

Alice

Bob

Cindy

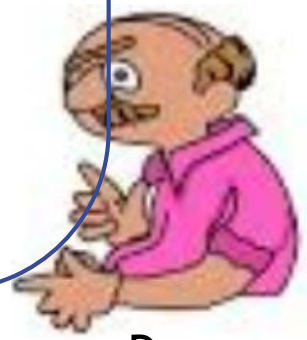
Dan

Bob付50BTC给Alice	Sha-256(“Bob付50BTC给Alice”)
Bob付20BTC给Dan	Sha-256(“Bob付20BTC给Dan”)

Alice

Bob

Cindy



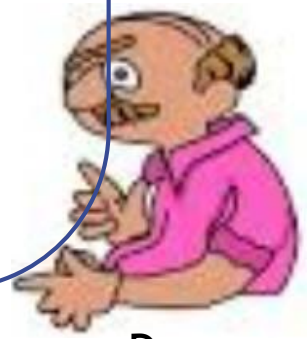
Dan

Bob付50BTC给Alice	Bob私钥加密(Sha-256(“Bob付50BTC给Alice”))
Bob付20BTC给Dan	Bob私钥加密(Sha-256(“Bob付20BTC给Dan”))

Alice

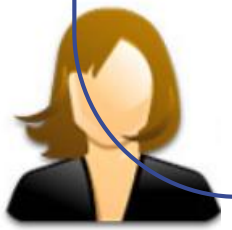
Bob

Cindy



Dan

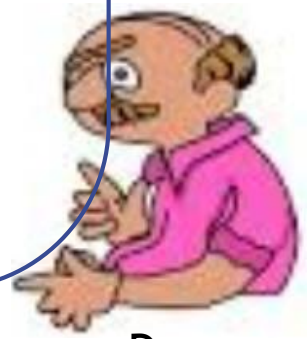
ID		
1	Bob付50BTC给Alice	Bob私钥加密(Sha-256(“Bob付50BTC给Alice”,id=1))
2	Bob付20BTC给Dan	Bob私钥加密(Sha-256(“Bob付20BTC给Dan”,id=2))
3		



Alice

Bob

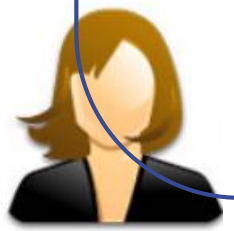
Cindy



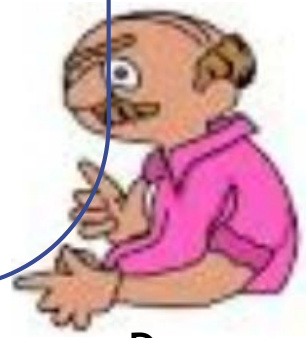
Dan

ID		
1	Bob付50BTC给Alice	Bob私钥加密(Sha-256(“Bob付50BTC给Alice”,id=1))
2	Bob付20BTC给Dan	Bob私钥加密(Sha-256(“Bob付20BTC给Dan”,id=2))
3	Bob付20BTC给Dan	Bob私钥加密(Sha-256(“Bob付20BTC给Dan”,id=2))

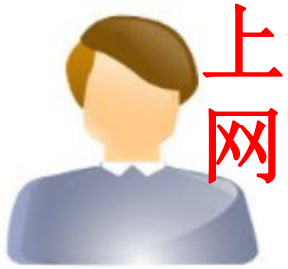
这样便确保了他人对某一个区块中数据的**不可篡改性**



Alice



Dan



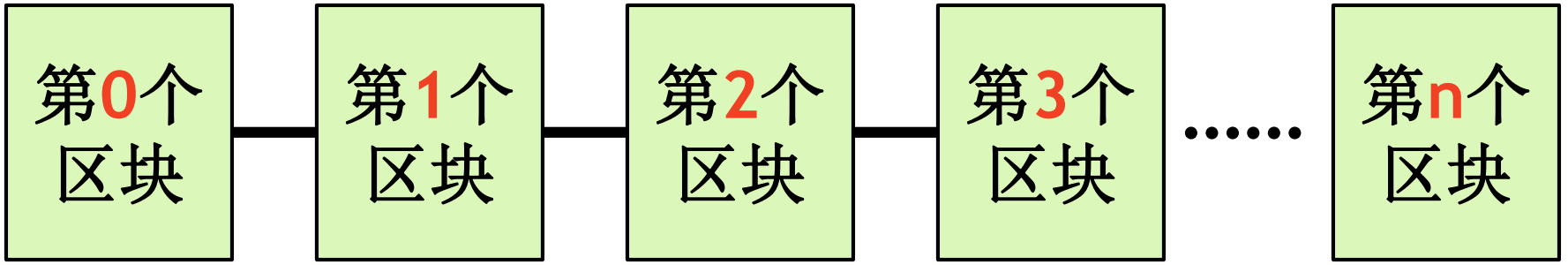
Bob

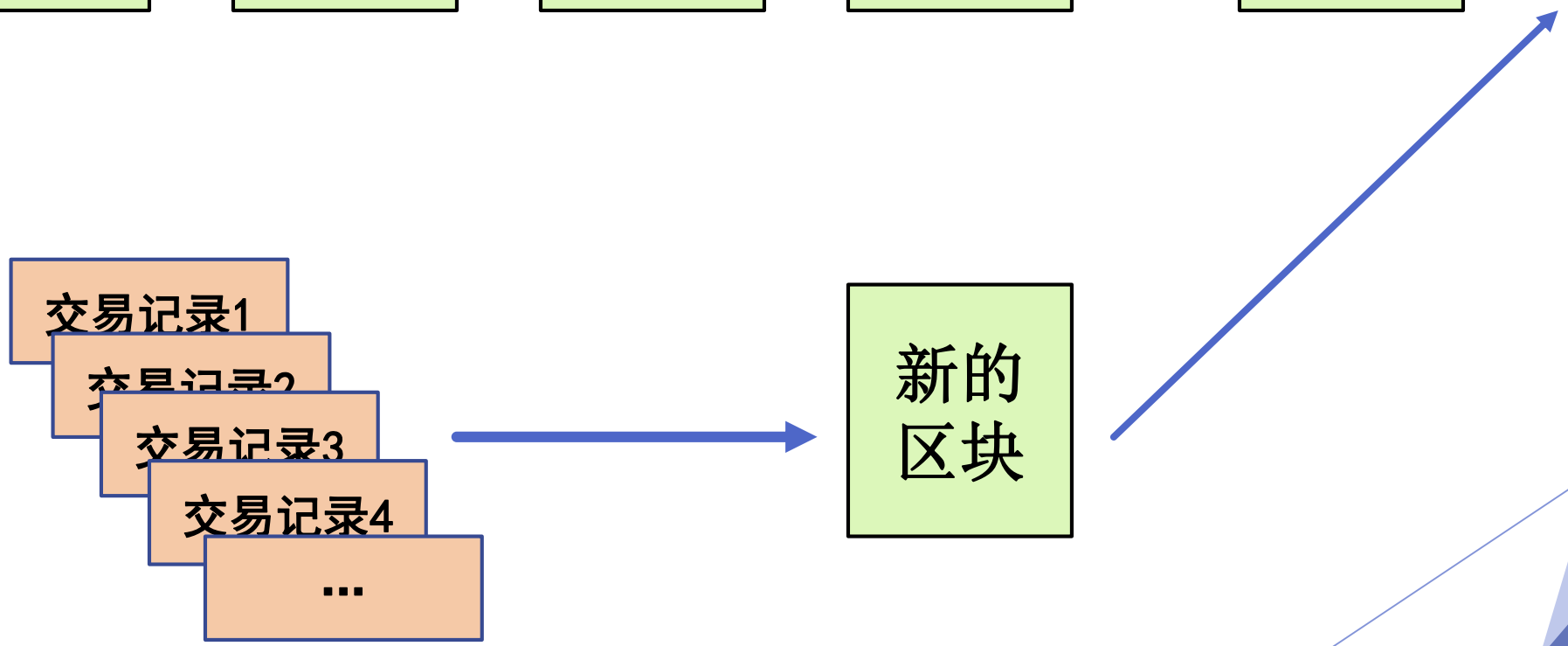
上述的账单 也就是比特币网络中的一个区块

Cindy

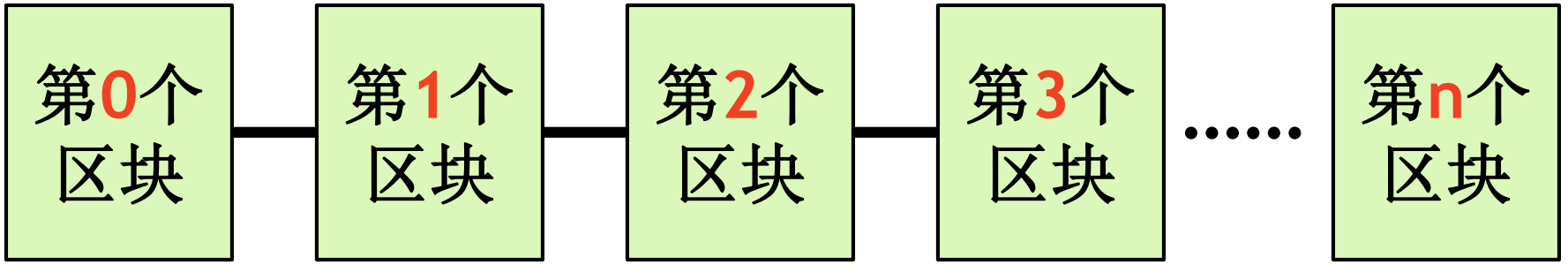
2.链式结构

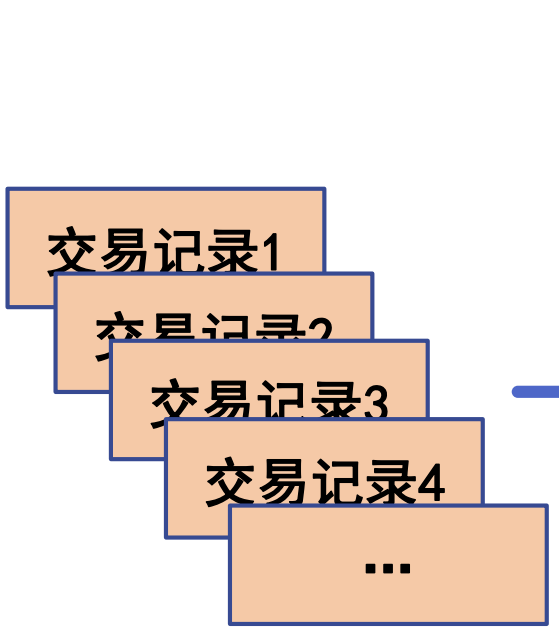
区块链：如何防止篡改？





区块链：

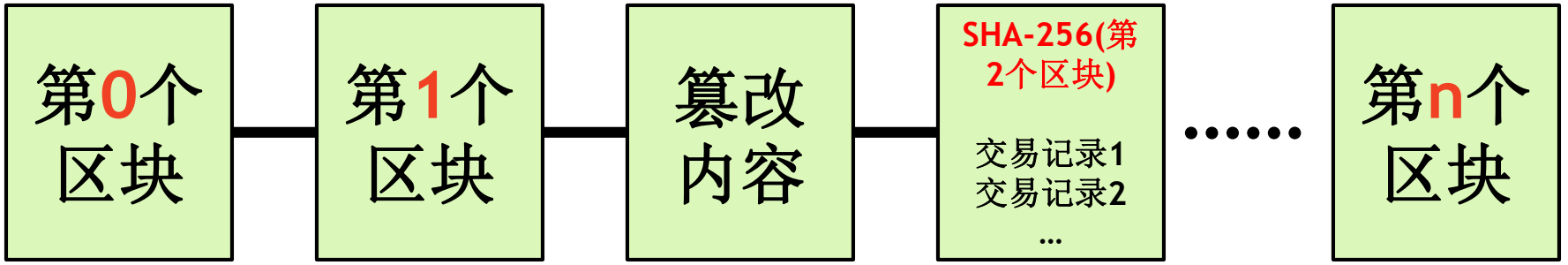


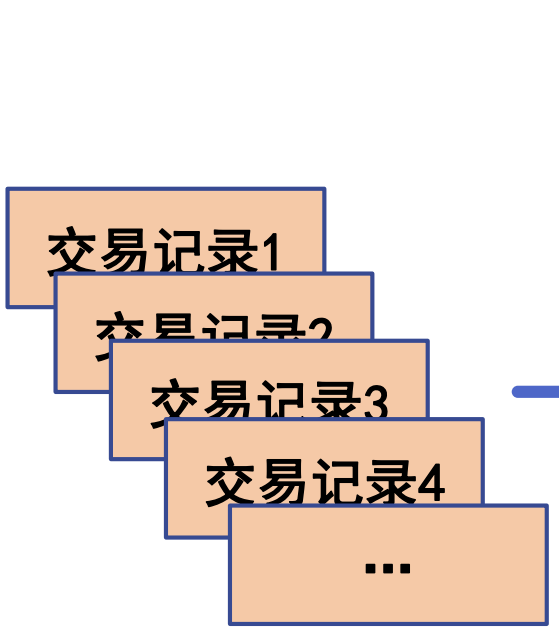


SHA-256(第n区块)

（非对称加密后的）
交易记录1
交易记录2
…

区块链：

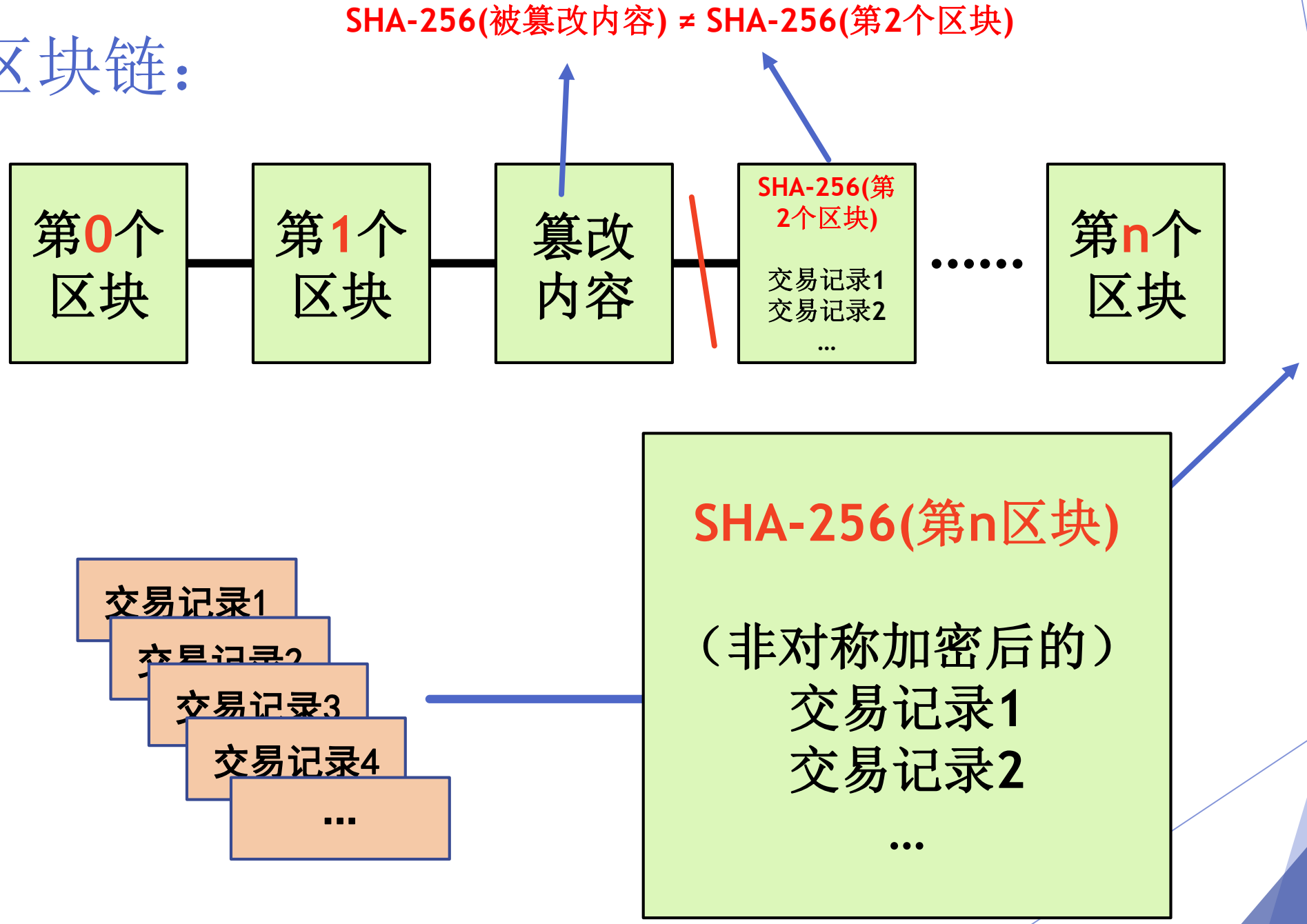




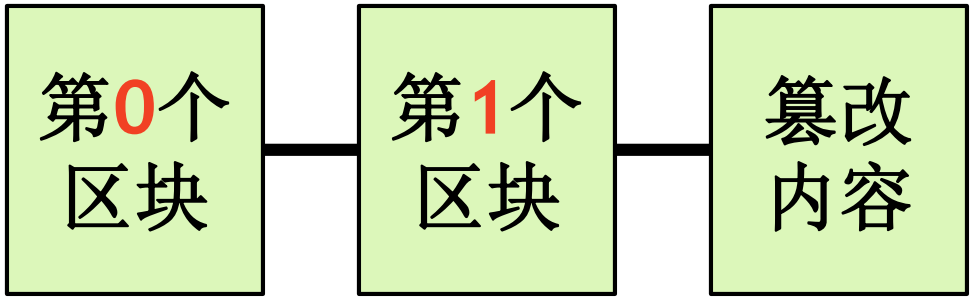
SHA-256(第n区块)

（非对称加密后的）
交易记录1
交易记录2
...

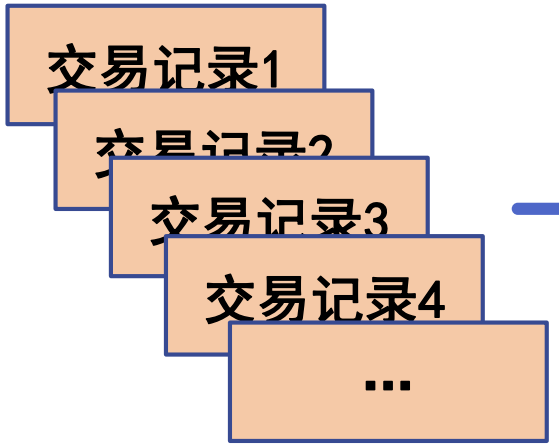
区块链：


SHA-256(被篡改内容) ≠ SHA-256(第2个区块)
第0个区块
第1个区块
篡改内容
SHA-256(第2个区块)
交易记录1
交易记录2
...
.....
第n个区块
交易记录1
交易记录2
交易记录3
交易记录4
...
SHA-256(第n区块)
（非对称加密后的）
交易记录1
交易记录2
...

区块链：



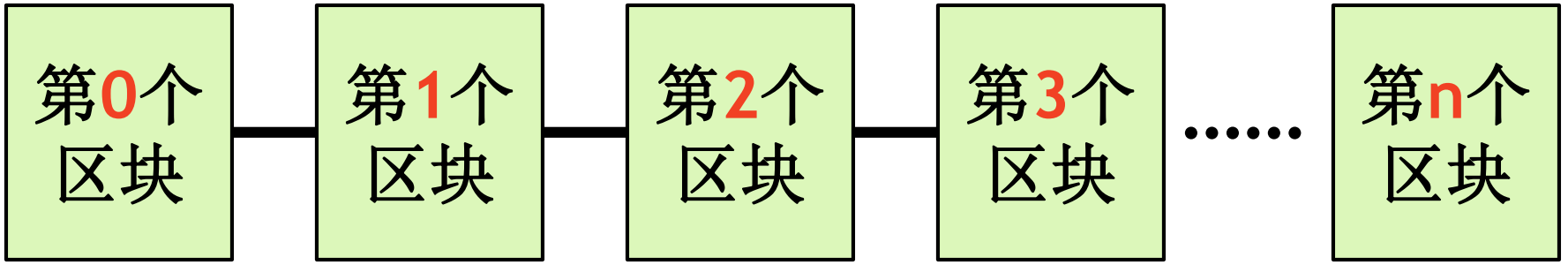
整条区块链直接断裂，
比特币网络不再认可
这条被篡改的链

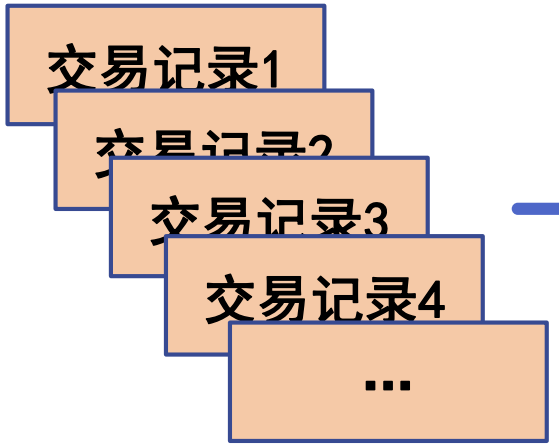


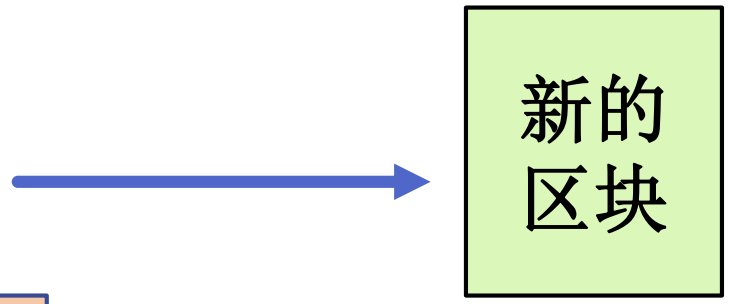
SHA-256(第n区块)

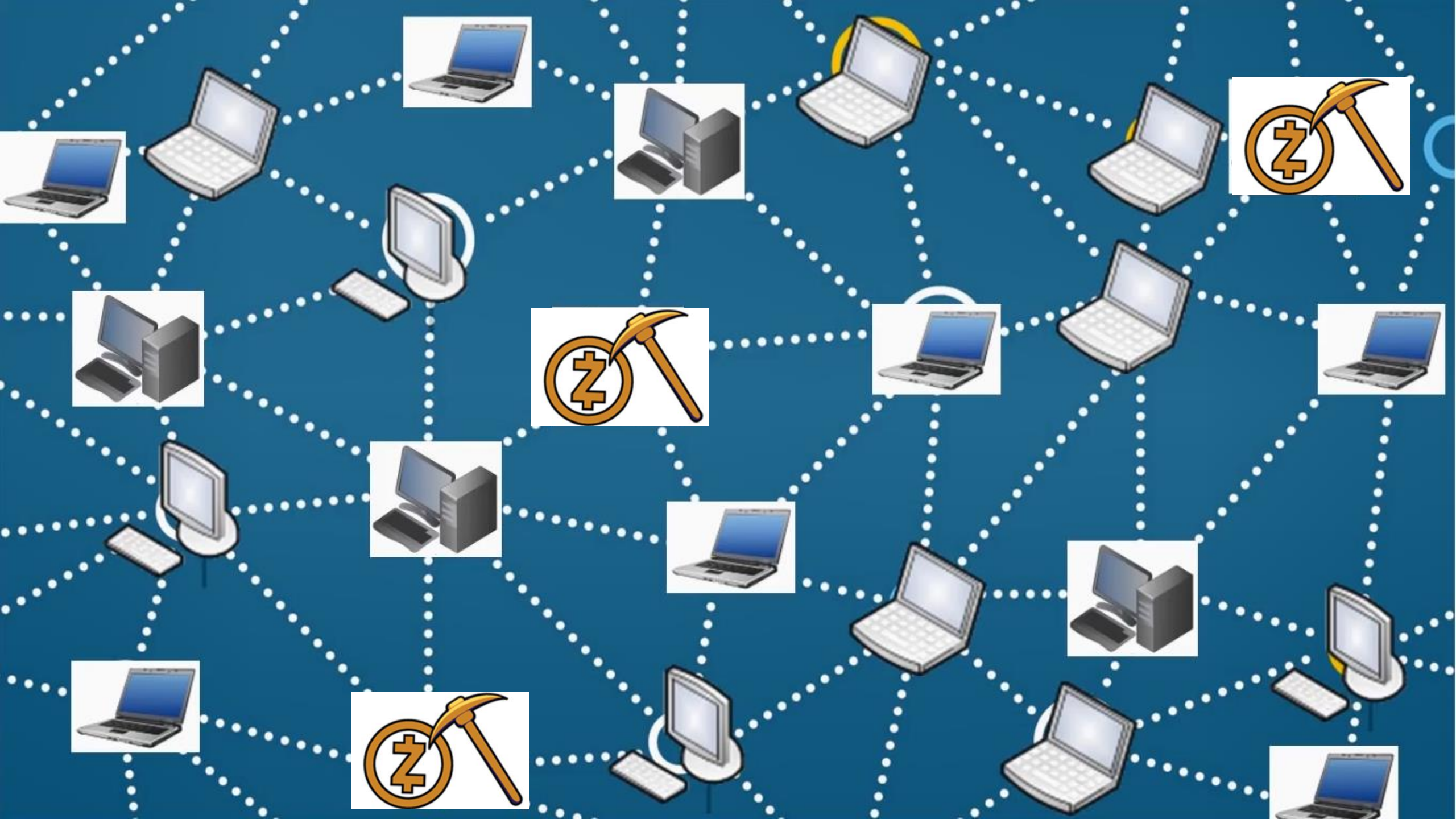
（非对称加密后的）
交易记录1
交易记录2
...

区块链：　每个新区块由谁生成？









1.负责收集比特币网络中的交易信息

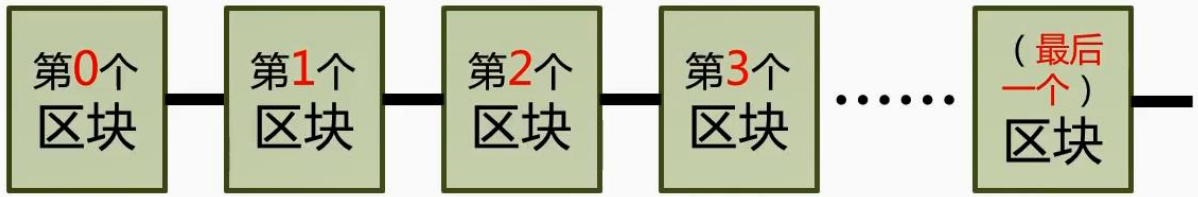
2.对上述信息进行处理
确认有效性

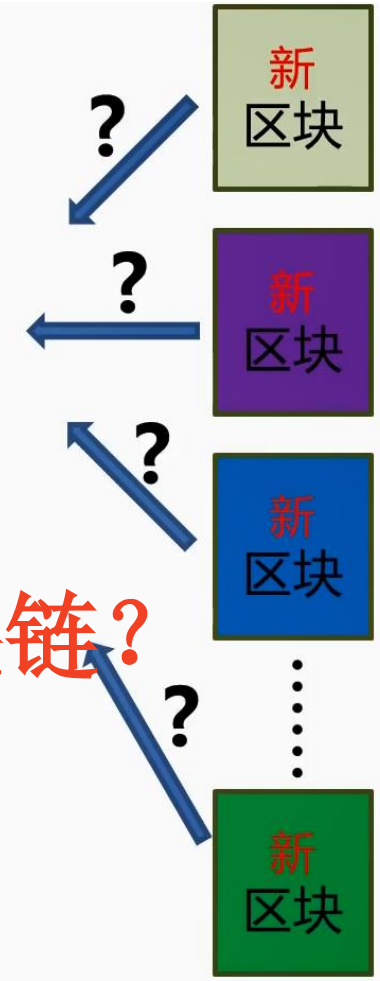
3.矿工获得该区块中
交易费(约2BTC)+12.5BTC(2017年数据)

约合人民币384120元

解决方案：采用一个巧妙的方法限制单位时间内生成的新区块的数量

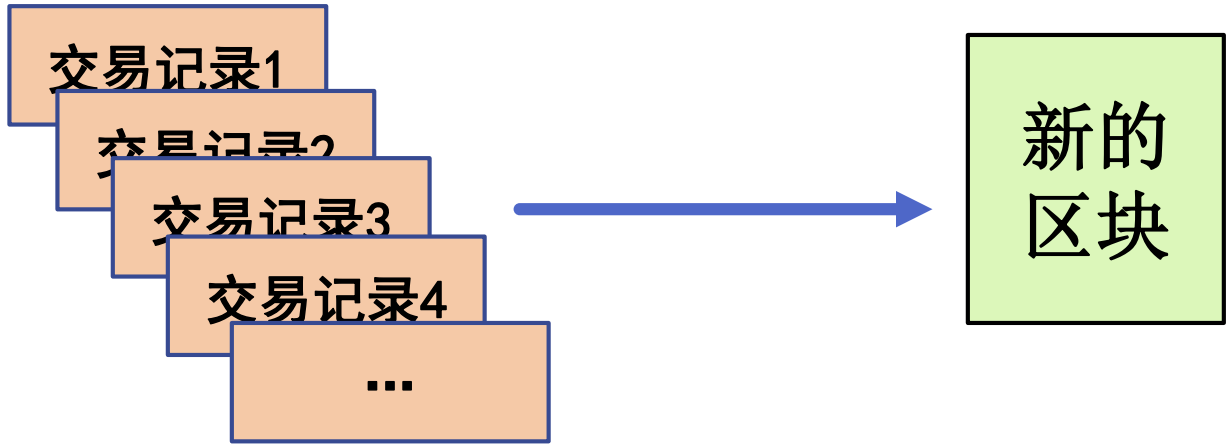
区块链：





如何保证最后生成的只是一条区块链？

巧妙的方法：



成功完成一个额外的工作后，才能把生成的区块发布到网络上

工作量证明(prove of work)

SHA-256（ SHA-256(上一个区块)

交易记录1
交易记录2
…

） =

10110110100101
11101110011001
00001011100101
11100001000101
11001100101111
01….
（共256位）

工作量证明(prove of work)

SHA-256（ SHA-256(上一个区块)

交易记录1
交易记录2
...
+随机数a

） =

10100101111000
01000101110011
00101111101101
00101111010000
11001000010111
01....
（共256位）

工作量证明(prove of work)

SHA-256（ SHA-256(上一个区块)

交易记录1
交易记录2
...
+随机数b ） =

10001000010111
00101110011001
01111111110110
10010111101000
01110010111110
01....
（共256位）

工作量证明(prove of work)

SHA-256（ SHA-256(上一个区块)

交易记录1
交易记录2
...
+随机数c

） =

11100000110110
00010010010100
01010001001100
00100001110000
11111100000100
00....
（共256位）

工作量证明(prove of work)

SHA-256（ SHA-256(上一个区块)

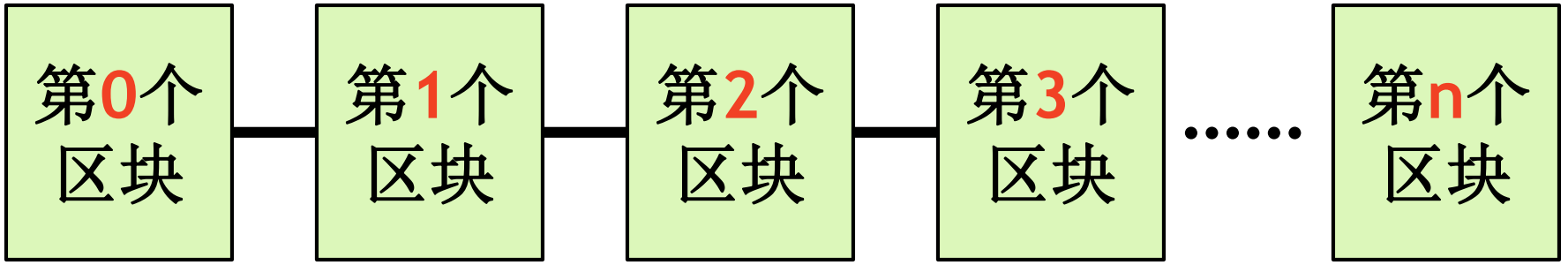
交易记录1
交易记录2
…
+随机数x ）=

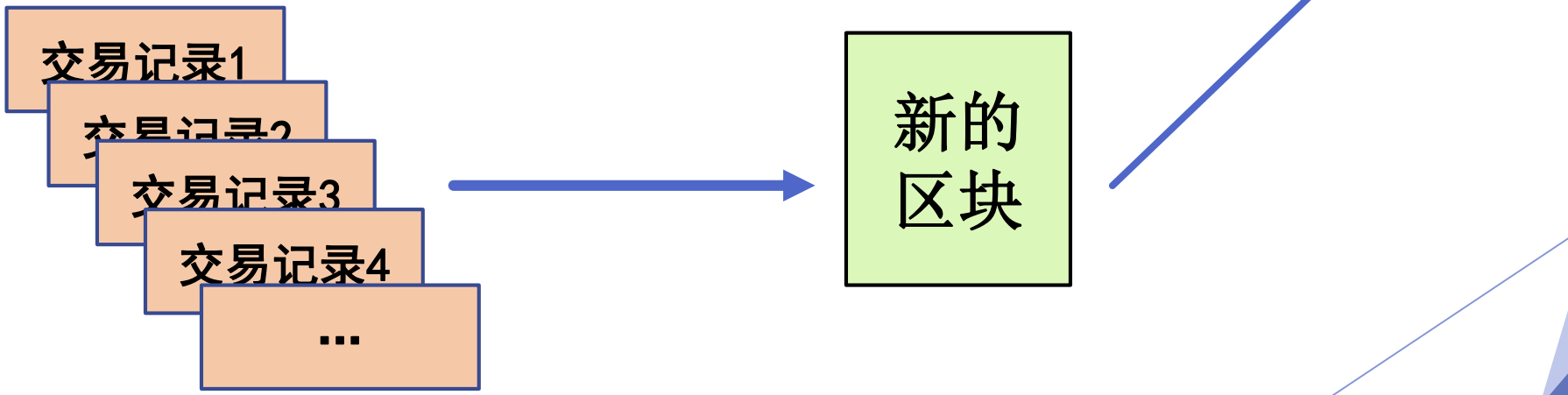
000000000000000
000000000000000
000000000000000
000000000000000
000000000000000
00....
（共256位）

前72位全为0

区块链：

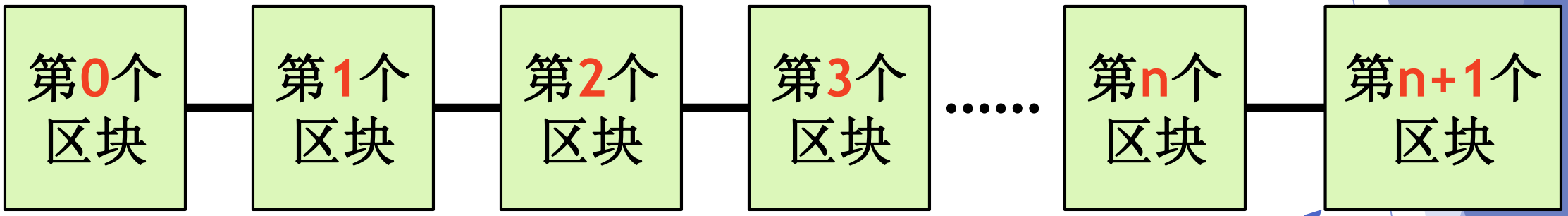
SHA-256(new block)=
000000000000000000000000000000000000
000000000000000000000000000000000.....



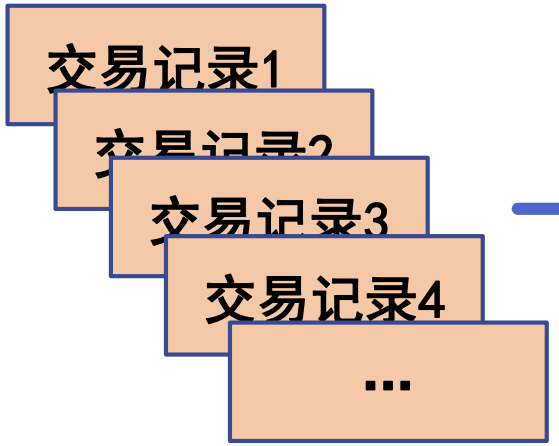


区块链：

SHA-256(new block)=
000000000000000000000000000000000000
000000000000000000000000000000000000.....



矿工寻找随机数的过程
我们称之为挖矿



前1位为0的概率：$\frac{1}{2}$

前2位为0的概率：$\frac{1}{2} \times \frac{1}{2}$

前n位为0的概率：$\frac{1}{2^n}$

n=72时

整个比特币网络平均需要计算

2^{72} ≈ 4.7×10^21次　SHA-256函数

才有可能得到一个能被比特币网络承认的区块

根据中本聪的设计，在整个比特币网络一般只有一个矿工能在十分钟左右时间内完成这个额外的工作

$2^{72} \approx 4.7\times10\text{^}21$次　是什么概念？

- 普通CPU的个人计算机 ： 6.0×10^{5} 次/秒
- 加装多个显卡的个人计算机： 1.0×10^{8} 次/秒
- 专业挖矿机：1.0×10^{13} 次/秒

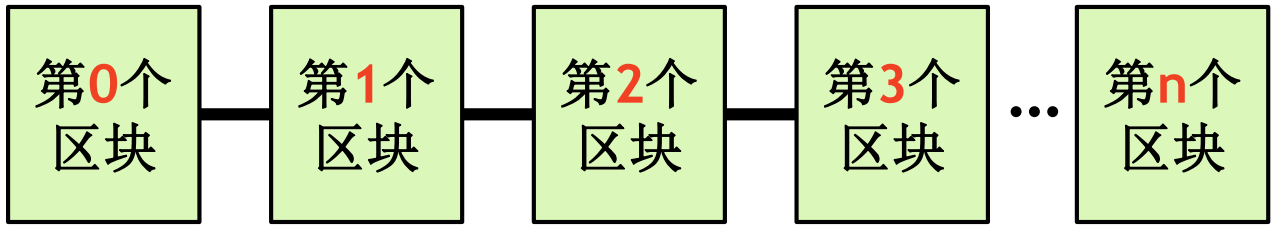
即便用一台专业挖矿机挖矿，大约需要挖15年才有可能挖到比特币

所以如今的挖矿，都是拼的运算速度，拼的手气。

同时，网络根据生成区块的平均时间来调整难度，使得区块的增长速度永远为10分钟

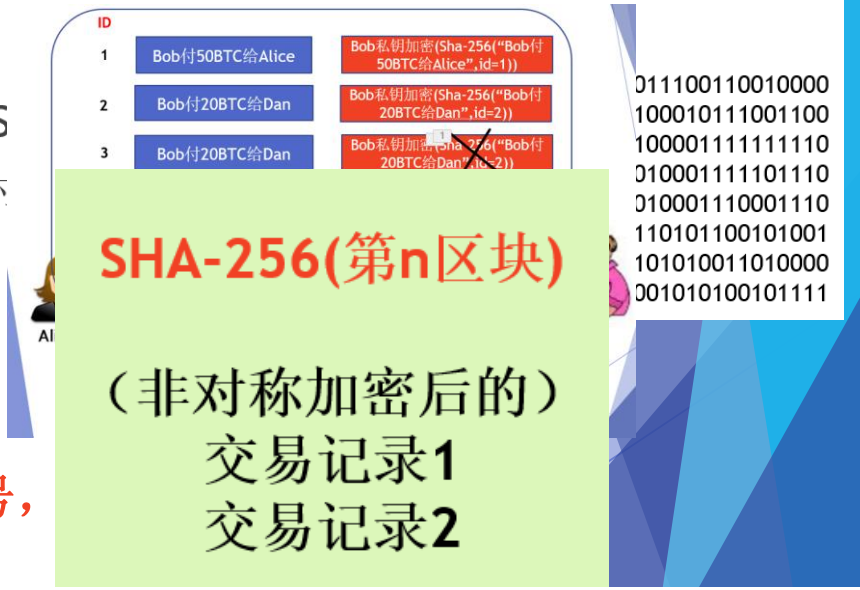
用算法建立起可靠的信用体系

区块链



一种按照时间顺序将数据区块以顺
的方式组合成的一种链式数据结构
密码学方式保证的不可篡改和不可
分布式账本。

哈希算法



不可篡改
- 哈希函数（SHA-256）
- 非对称加密算法，并加上编号，

链式结构
- 在区块头部加入上一个区块的特征信息（哈希值）
- 工作量证明
- 定期调整挖矿难度

整个比特币网络平均需要计算 $2^{72} \approx 4.7\times10^{21}$次 SHA-256函数

谢谢！

参考资料：

- 1. https://bitcoin.org/bitcoin.pdf

  Bitcoin: A Peer-to-Peer Electronic Cash System

  （比特币：一种对等式电子货币系统） ----中本聪

- 2. https://www.youtube.com/watch?v=obRzfcvMshM&t=622s

  比特币原理 ---- Junqiang Jin