Blockchain
区块链

2018.03.13

区块链技术

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

课堂测试时间

课堂测试01

- 1、简单描述区块链是如何防止篡改的?
- 2、简单描述公钥作为身份的好处?
- 3、简单描述随机性在比特币的分布式共识机制中的作用?
- 4、如果恶意ISP完全控制用户的网络链路，是否能发起针对该用户的双重支付？需要多少计算量?
- 5、简单介绍区块链的5个基本原则?
- 6、简单分析TCP/IP发展和区块链发展的异同，借鉴论文方法和思想，你预测一下区块链2020年、2030年、2040年的发展，简单分析理由。

上次课程内容回顾

- 密码学
- 加密货币
- 对等网络
- 去中心化

- 对称密码学、非对称密码学、PKI、PGP
- Hash函数、加密Hash函数、Hash指针、梅克尔树、数字签名、公钥做为身份
- 高飞币、贪心币
- 去中心化：技术 vs. 经济
- 拜占庭将军问题，分布共识、隐形共识

Projects

Projects

课程项目

- 选择一个区块链应用相关的项目(平台类项目不行，必须是具体的应用类项目)，每位同学一个，不能重复，发到课程群，格式：学号－姓名－项目名称－应用领域；先到先得。应用领域可以不准确
- 每个同学完成自己的项目总结报告，总结报告要分析该项目的发展历程、发展趋势、优缺点、面临问题，你的所思所想；
- 根据项目对同学进行分组，每个组对应一个区块链相关的应用领域；
- 每个组完成该应用领域总结报告；总结报告要分析该领域的发展历程、发展趋势、优缺点、面临问题，小组讨论后的所思所想；
- 小组提出一个新的项目设计，撰写完成项目白皮书；
- 最后一次课前提交项目总结报告、项目白皮书和报告PPT，最后一次课报告 (具体时间待定)；
- 所有参考资料、完成文档和PPT等上传Github。

本周日提交每个人项目选题

区块链Demo

Fork me on GitHub

kchain Demo Hash Block Blockchain Distributed Tokens Coinbase

Blockchain Demo – Part 1

https://anders.com/blockchain/

Blockchain 101 - A Visual Demo

Hash Block Blockchain Distributed Tokens Coinbase

Blockchain

3	Block: # 4	Block: # 5
37	Nonce: 35990	Nonce: 56265
	Data:	Data:
012fa9b916eb9078f8d98a7864e697ae83	Prev: 0000b9015ce2a08b61216ba5a0778545bf4d	Prev: 0000ae8bbc96cf89c68be6e10a865cc47c6c4
0b9015ce2a08b61216ba5a0778545bf4d	Hash: 0000ae8bbc96cf89c68be6e10a865cc47c6c4	Hash: 0000e4b9052fd8aae92a8afda42e2ea0f1797
	Mine	Mine

密码学学习

Subjects ▾ Search KHANACADEMY

‹ COMPUTER SCIENCE

Journey into cryptography

CONTENTS

How have humans protected their secret messages through history? What has changed today?

Ancient cryptography

Explore how we have hidden secret messages through history.

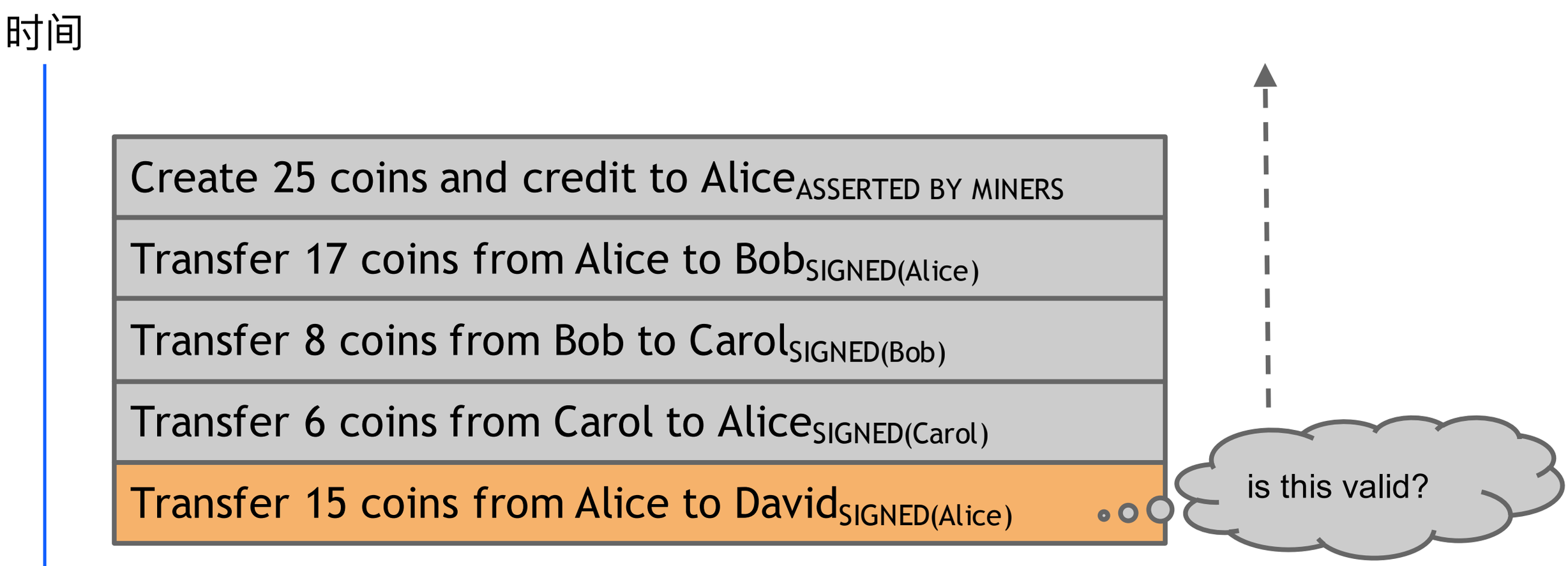
- What is cryptography?
- The Caesar cipher
- Caesar Cipher Exploration

https://www.khanacademy.org/computing/computer-science/cryptography

上次没讲完部分

交易

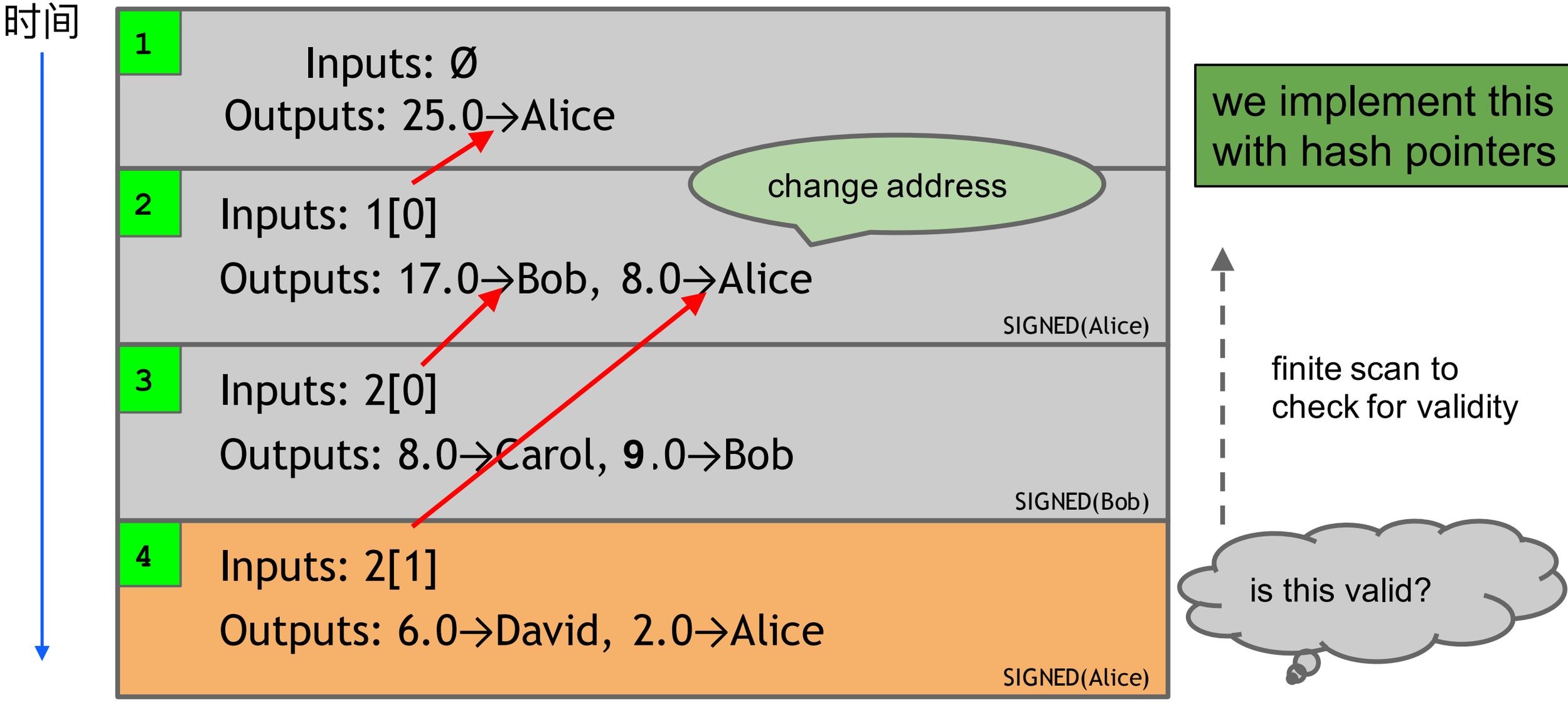
普通账本



一个块包含一个交易

交易验证需要扫描以前所有的块

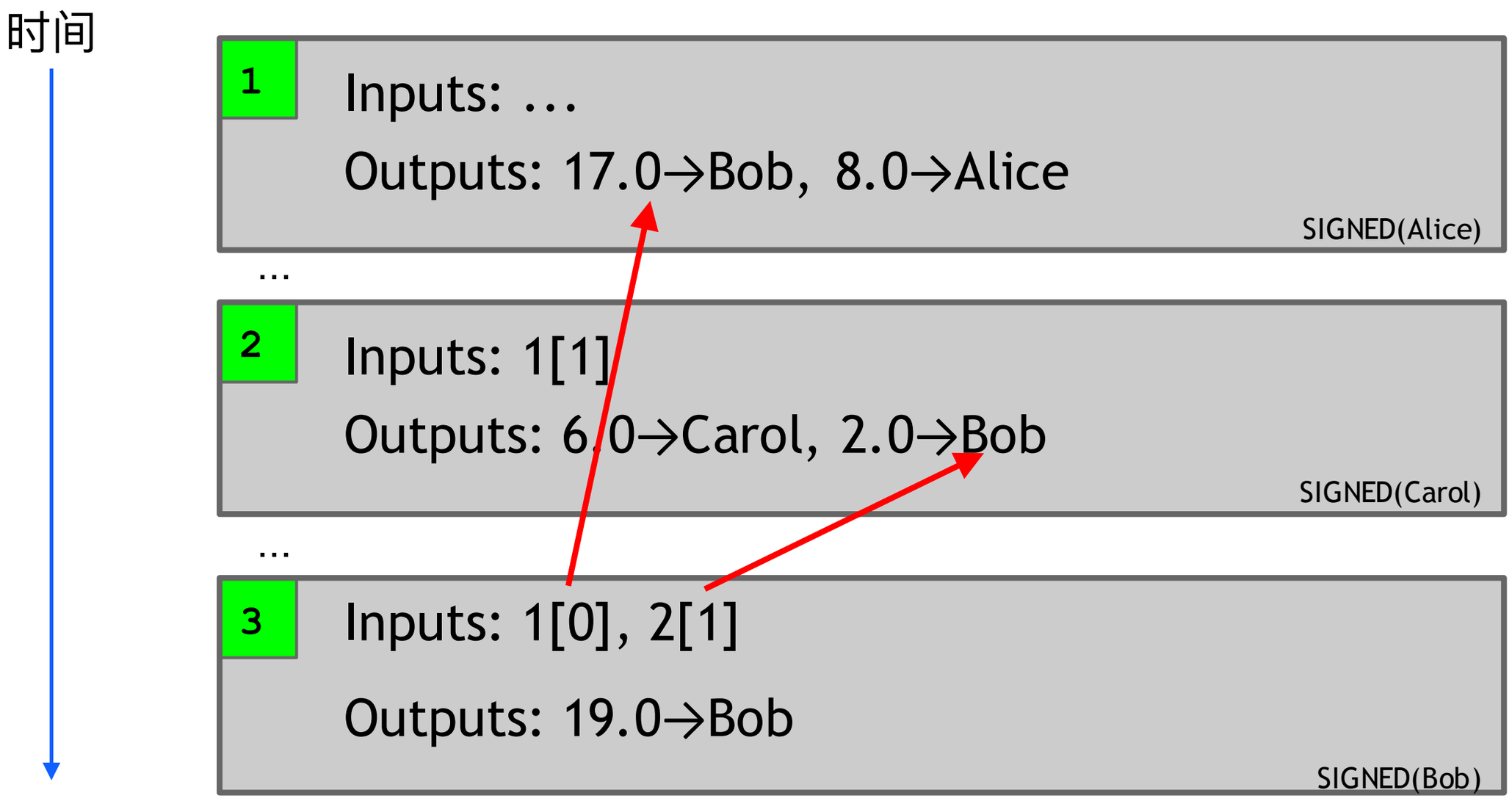
比特币



一个块包含一个交易

交易验证需要扫描以前所有的相关块

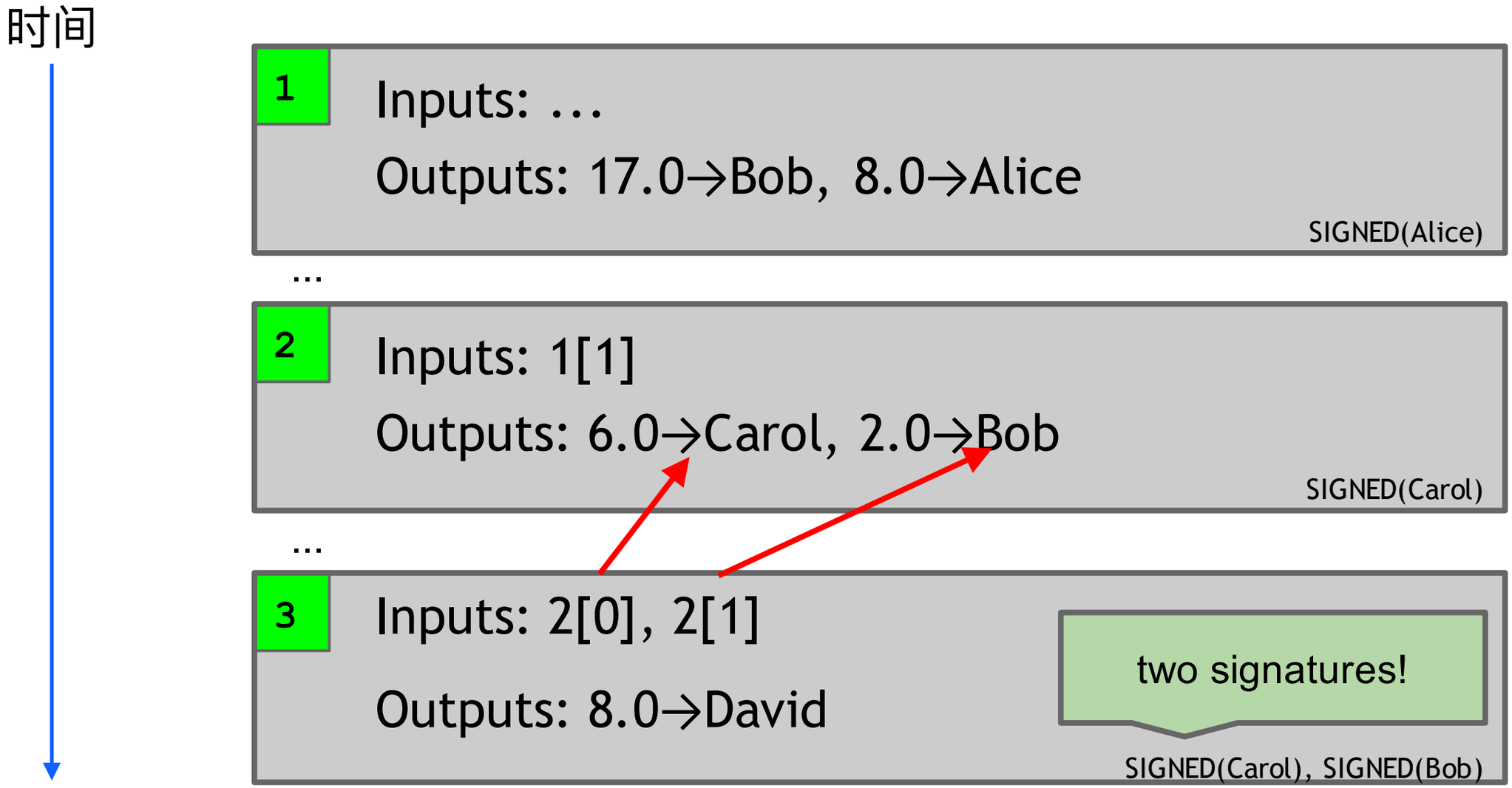
合并



一个块包含一个交易

交易验证需要扫描以前所有的相关块

联合支付



一个块包含一个交易

脚本

比特币交易

元数据

```
{
  "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
  "ver":1,
  "vin_sz":2,
  "vout_sz":1,
  "lock_time":0,
  "size":404,
```

输入

```
  "in":[
   {
      "prev_out":{
      "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
      "n":0
     },
       "scriptSig":"30440..."
   },
   {
      "prev_out":{
      "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
      "n":0
     },
     "scriptSig":"3f3a4..."
   }
  ],
```

输出

```
  "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

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
```

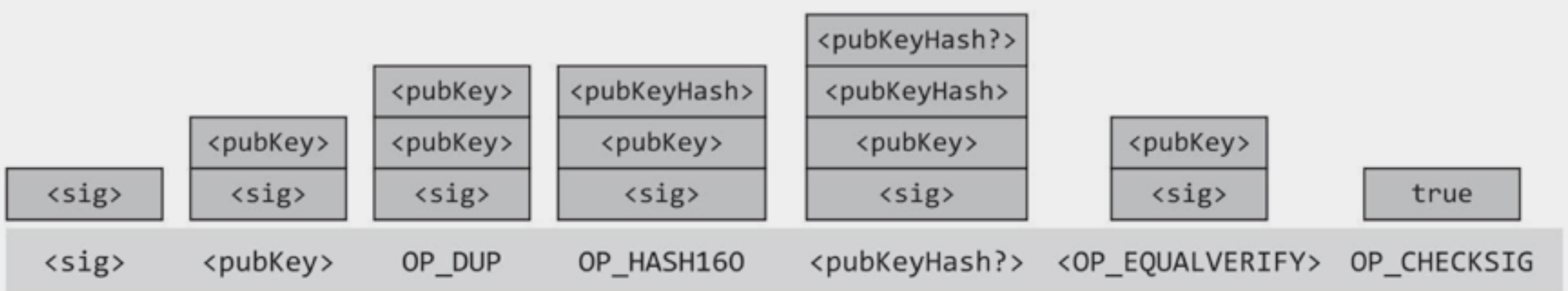


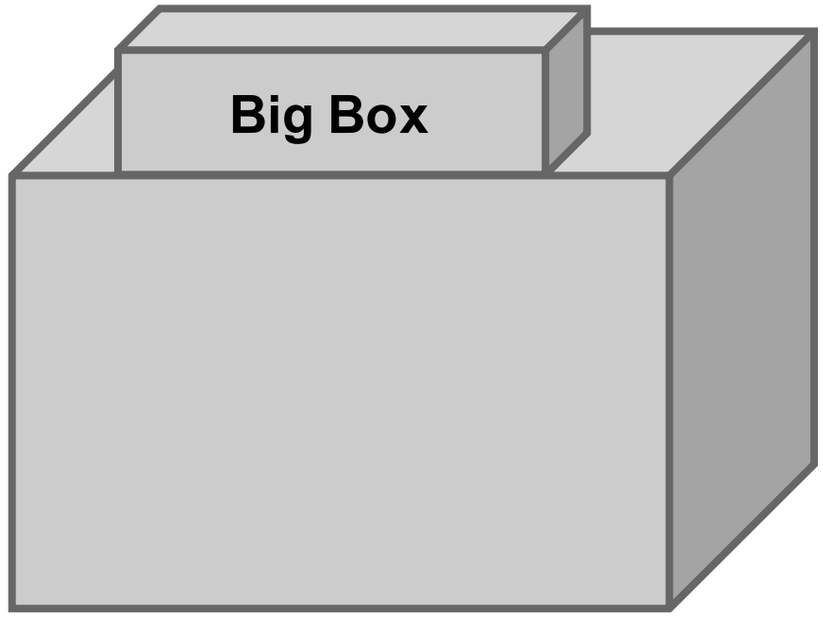
图3.6 比特币脚本的执行堆栈状态图

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。

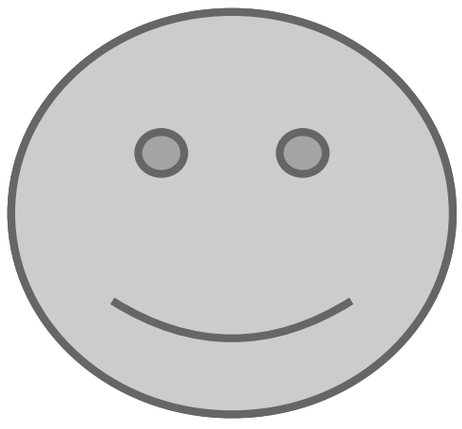
多重签名问题

I'm ready to pay for my purchases!

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!

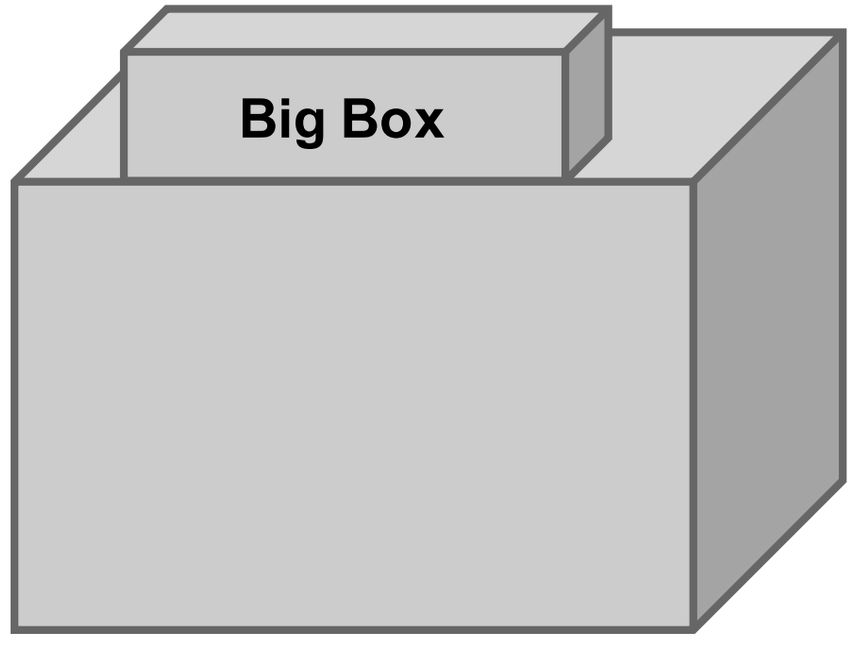


Pay for Script

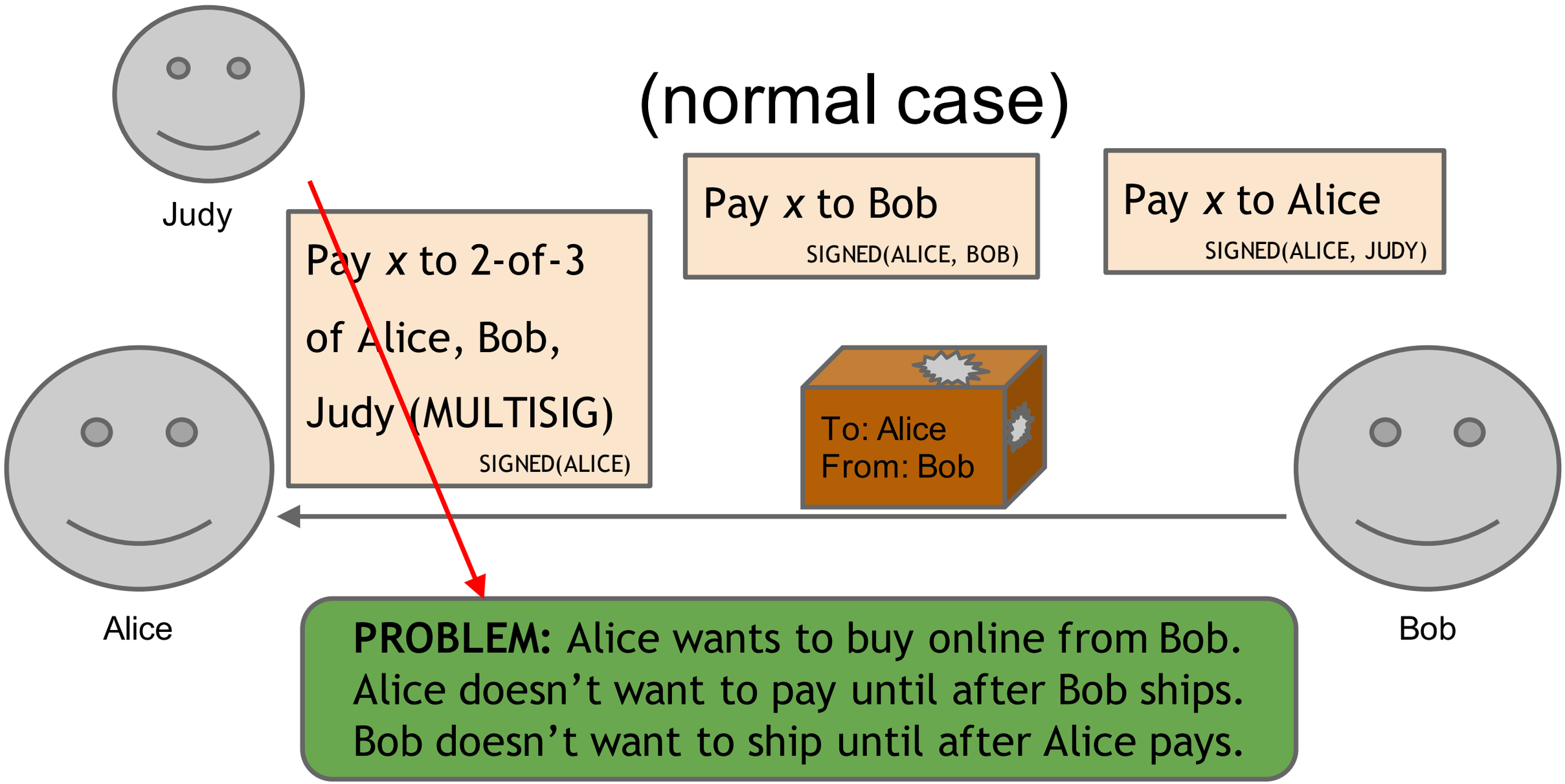


I'm ready to pay for my purchases!

Great! Here's our address: 0x3454



托管


(normal case)
Judy
Pay x to 2-of-3
of Alice, Bob,
Judy (MULTISIG)
SIGNED(ALICE)
Pay x to Bob
SIGNED(ALICE, BOB)
Pay x to Alice
SIGNED(ALICE, JUDY)
To: Alice
From: Bob
Alice
Bob
PROBLEM: Alice wants to buy online from Bob.
Alice doesn't want to pay until after Bob ships.
Bob doesn't want to ship until after Alice pays.

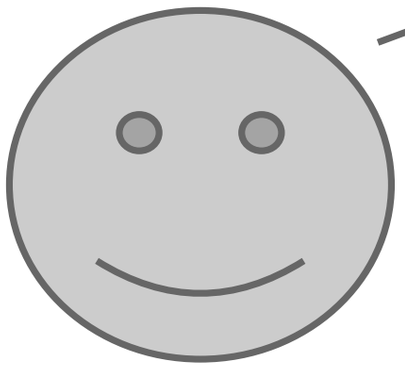
绿色地址

It's me, Alice! Could you make out a green payment to Bob?

Bank

004 days since last double spend!

Faraday cage

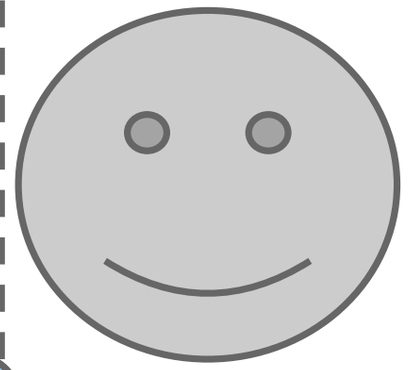


Alice

Pay x to Bob, y to Bank

No double spend

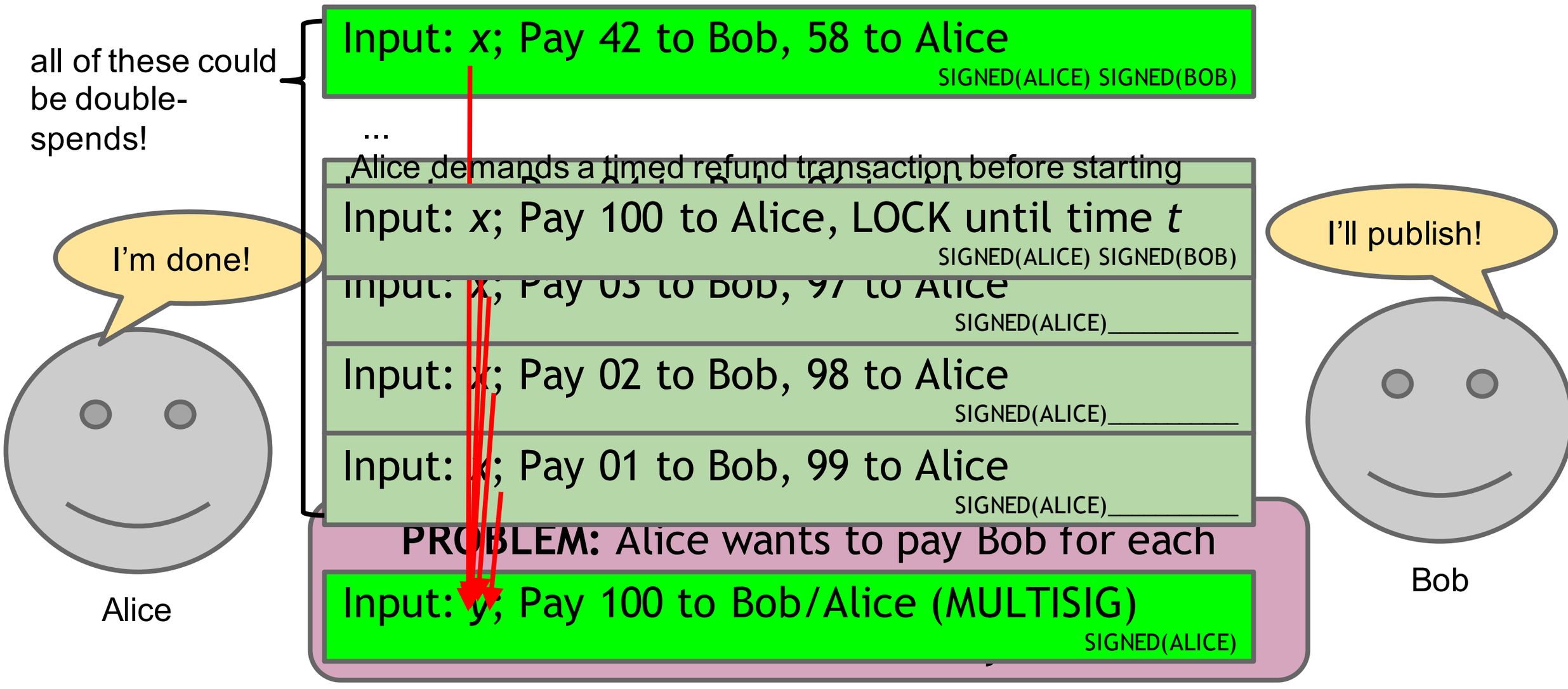
SIGNED(BANK)



Bob

PROBLEM: Alice wants to pay Bob.
Bob can't wait 6 verifications to guard against double-spends, or is offline completely.

小额多次交易


all of these could be double-spends!
Input: x; Pay 42 to Bob, 58 to Alice
SIGNED(ALICE) SIGNED(BOB)
...
Alice demands a timed refund transaction before starting
Input: x; Pay 100 to Alice, LOCK until time t
SIGNED(ALICE) SIGNED(BOB)
Input: x; Pay 03 to Bob, 97 to Alice
SIGNED(ALICE)
Input: x; Pay 02 to Bob, 98 to Alice
SIGNED(ALICE)
Input: x; Pay 01 to Bob, 99 to Alice
SIGNED(ALICE)
PROBLEM: Alice wants to pay Bob for each
Input: y; Pay 100 to Bob/Alice (MULTISIG)
SIGNED(ALICE)
I'm done!
I'll publish!
Alice
Bob

锁定时间


```
{
    "hash":"5a42590...b8b6b",
      "ver":1,
      "vin_sz":2,
      "vout_sz":1,
      "lock_time":315415,
      "size":404,
...
}
```


Block index or real-world timestamp before which this transaction can’t be published

区块

比特币的区块结构

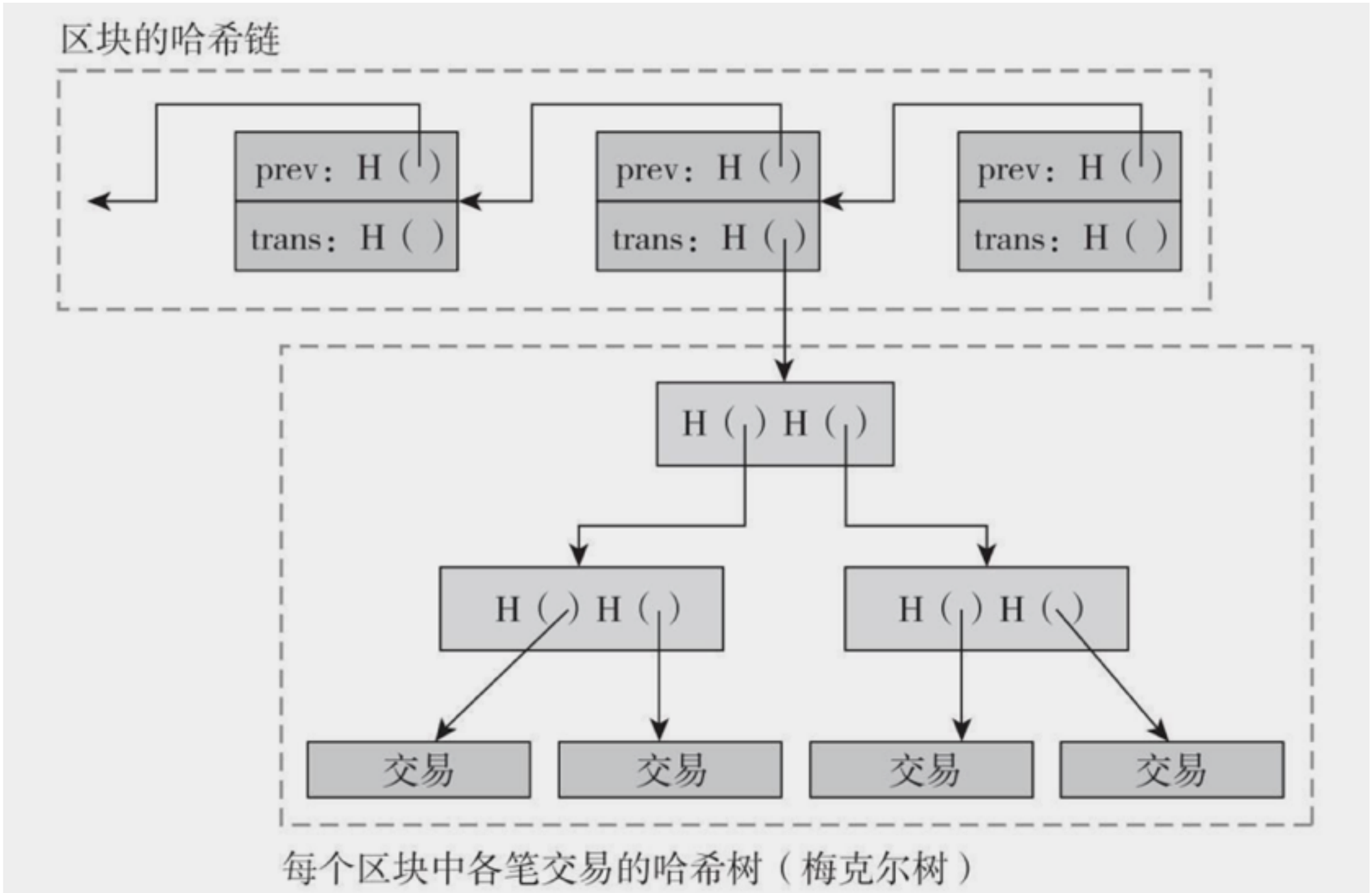


图3.7 比特币的区块链有两个哈希结构

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。

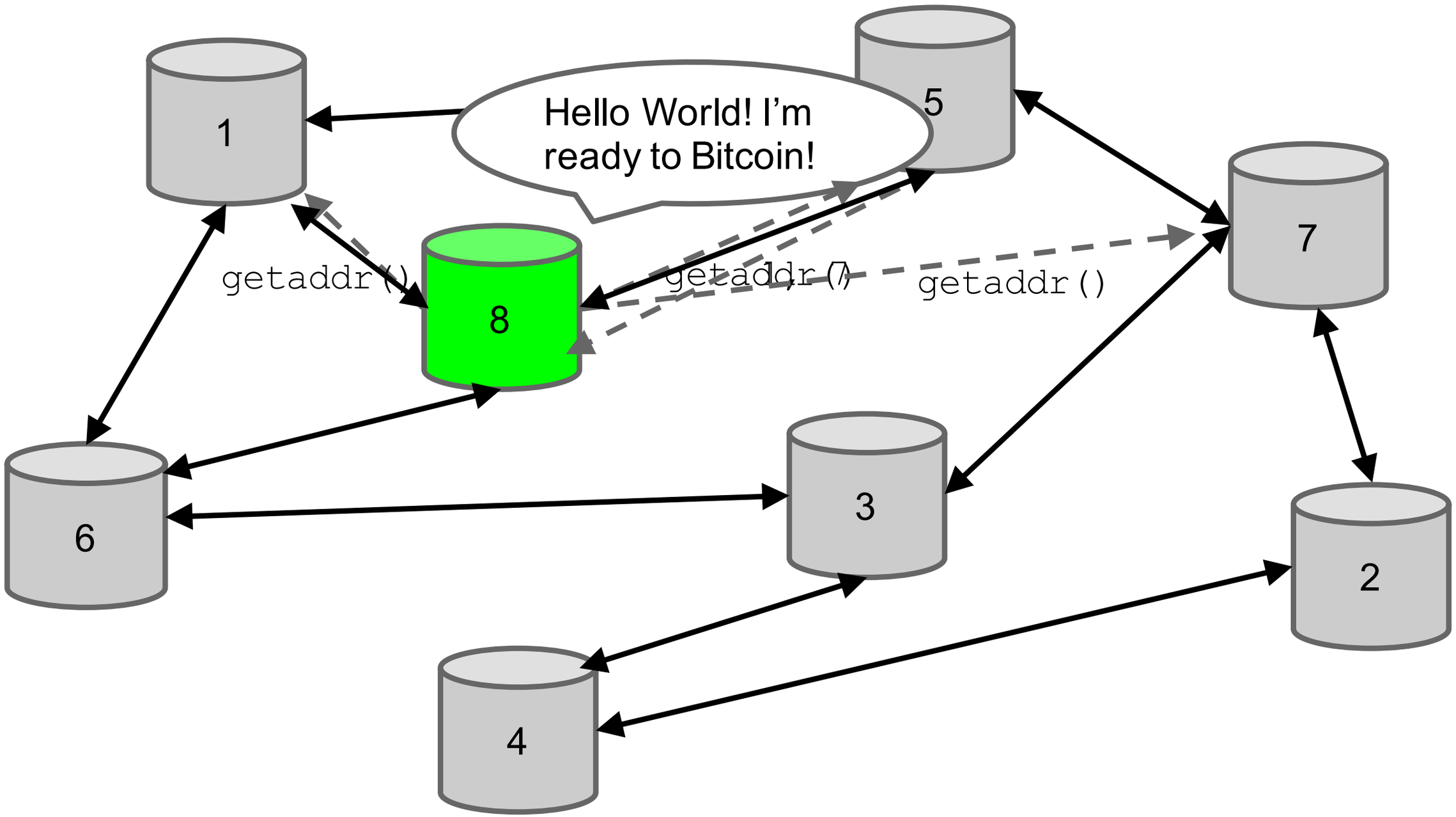
币基交易

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

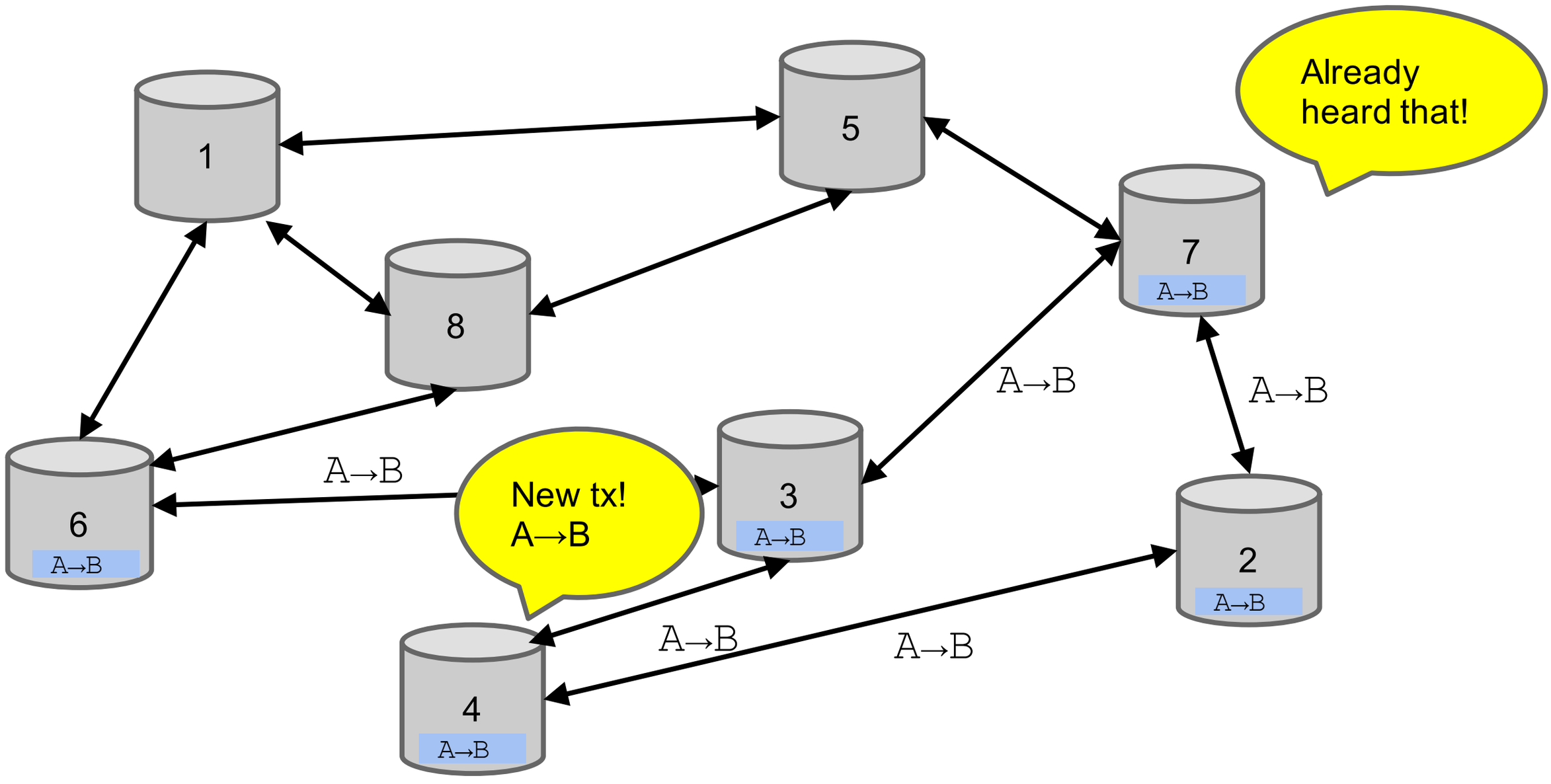
图3.8 币基交易

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



块传播

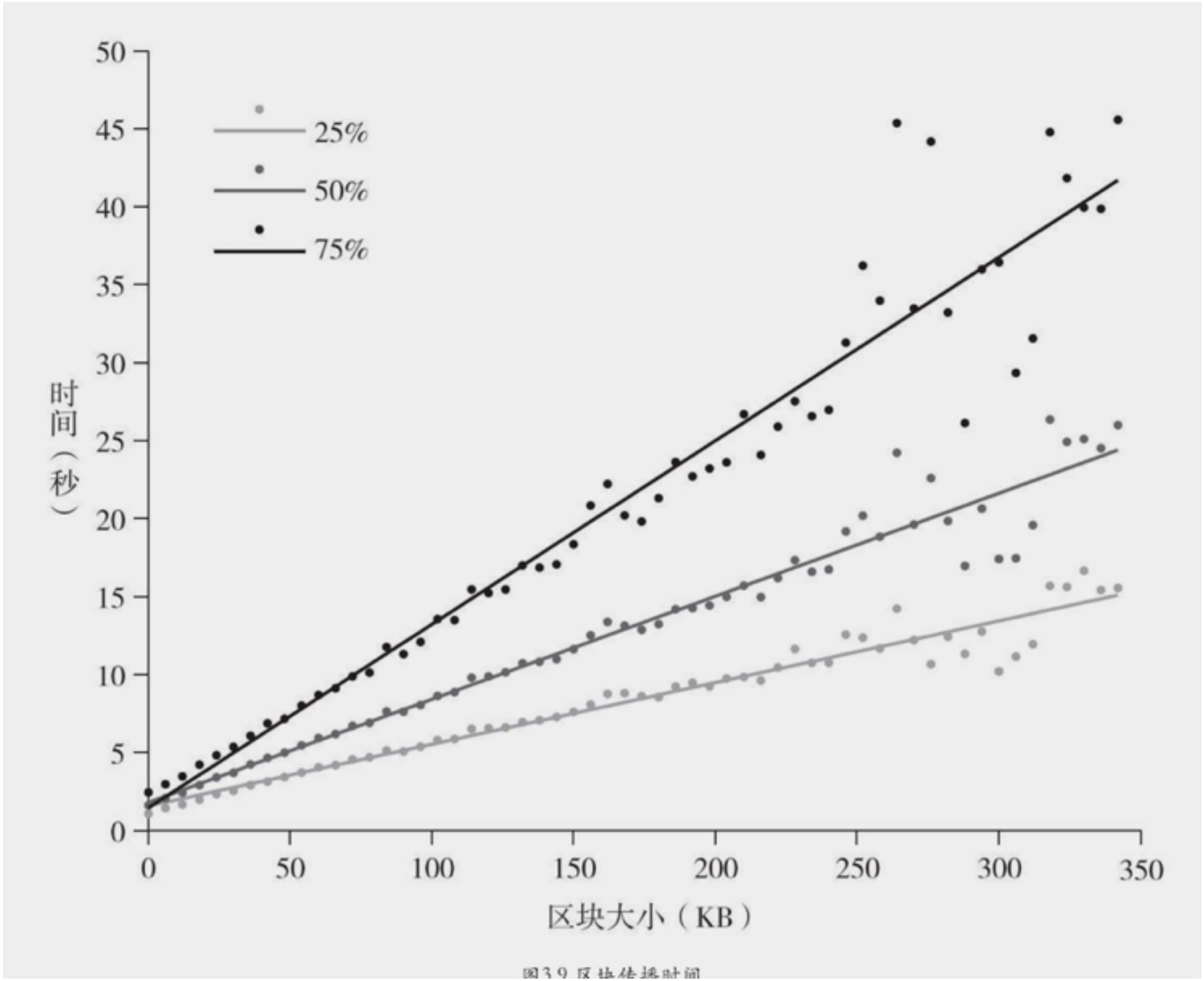


图3.9 区块传播时间

存储花费

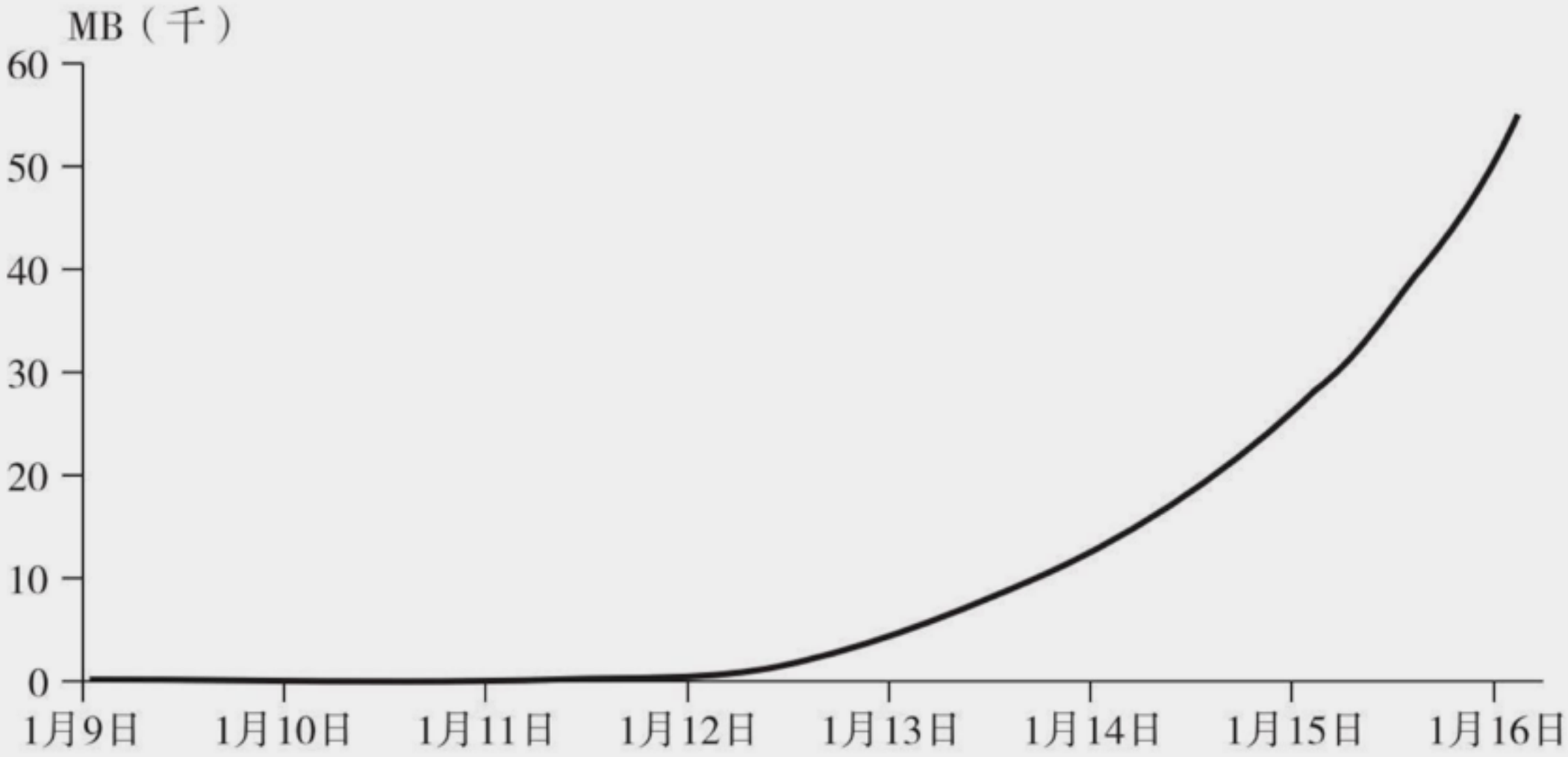


图3.10 区块链的大小

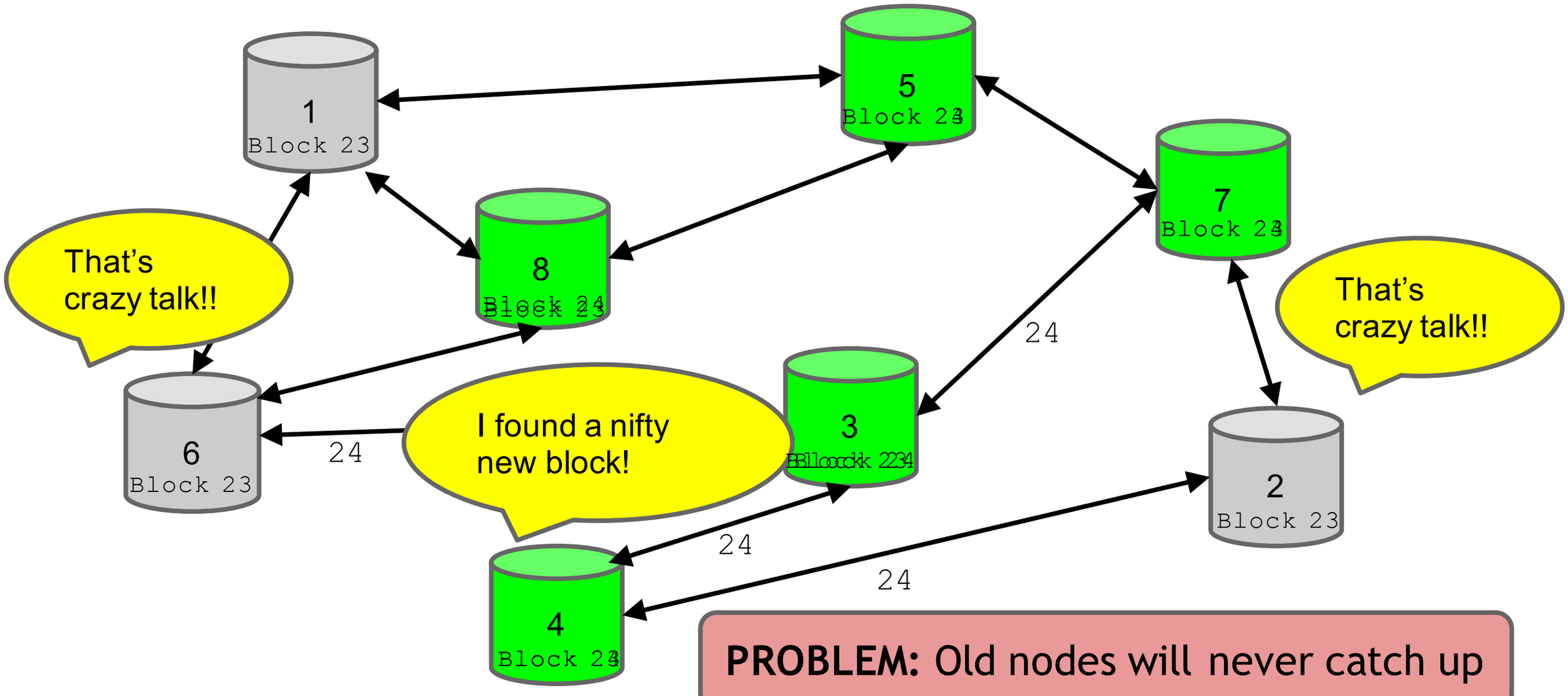
注：全节点必须保持整个区块链，在2015年年底，区块链大小在50GB以上。

限　制

比特币限制

- *10*分钟：产生块的间隔
- *1M*：一个块大小
- 2万签名：每个块
- *100M satoshi*：每个币
- *21M*：比特币数量
- *50*、*25*、*12.5*….：挖矿奖励
- *250bytes*：每个业务
- *7*交易：每秒*(visa 2*千到*1*万，*Paypal 50-100)*

分叉


1
Block 23
5
Block 24
7
Block 24
8
Block 24
That's crazy talk!!
24
That's crazy talk!!
6
Block 23
24
I found a nifty new block!
3
Block 24
2
Block 23
24
24
4
Block 24
PROBLEM: Old nodes will never catch up

硬 *vs.* 软

存储

比特币存储

Hot storage

online

hot secret key(s)

cold address(es)

payments

Cold storage

offline

威胁

Charles Ponzi

交易所


東京でMT.GOXのデモ
へ参加してください。
東京都渋谷区渋谷
2丁目11-5
MTGOX
WHERE IS
OUR MONEY
VAIO

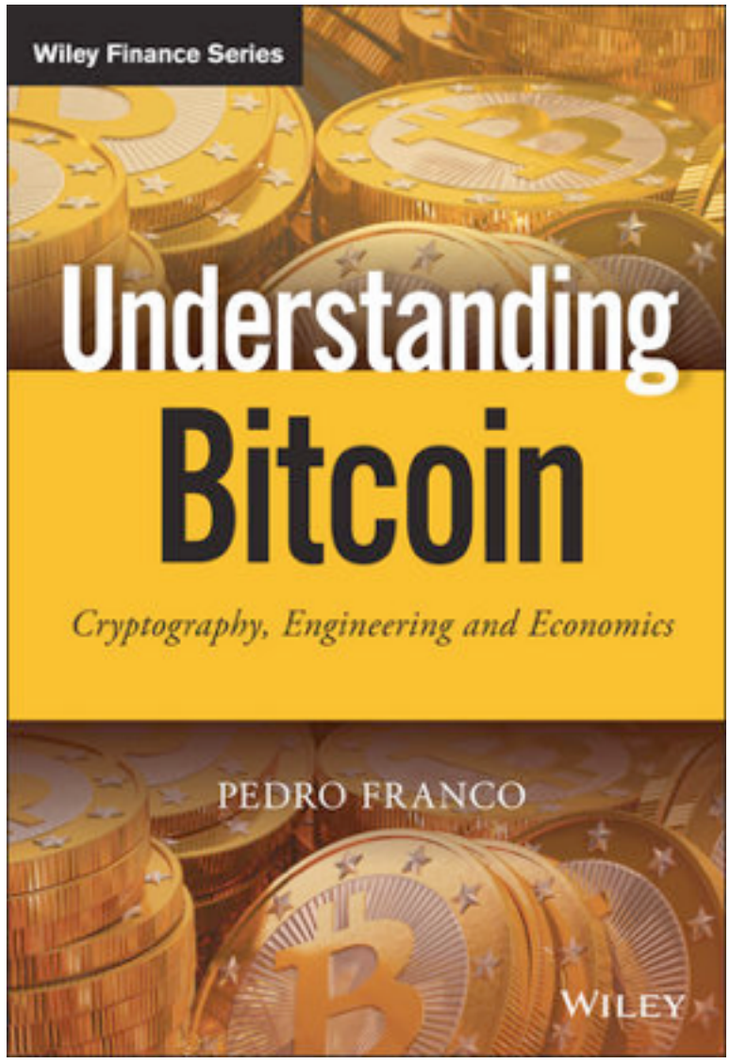
提问时间！

Home work

Homework

课后作业

第三章、第四章



第六章、第八章

Homework

课后作业

- 要求阅读如下论文，写论文阅读报告：

➡ *In IEEE Computer Maganize 2017.*

COVER FEATURE **BLOCKCHAIN TECHNOLOGY IN FINANCE**

The Evolution of Bitcoin Hardware

Michael Bedford Taylor, University of Washington

谢谢！

孙惠平

sunhp@ss.pku.edu.cn