

2018.03.13

区块链技术

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
 - 对称密码学、非对称密码学、PKI、PGP
- 加密货币
 - 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
- 对等网络
 - 高飞币、贪心币
- 去中心化
 - 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

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

Blockchain Technology

区块链Demo



Blockchain Demo – Part 1

<https://anders.com/blockchain/>

The screenshot shows a blockchain visualization with two main sections. On the left, a vertical stack of three light green rectangular blocks displays the numbers '3', '37', and 'e'. To the right, two horizontal light green rectangular blocks represent blocks 4 and 5. Each block has fields for 'Block', 'Nonce', 'Data', 'Prev', and 'Hash'. A large play button is centered between the two blocks.

Block:	#	4
Nonce:	35990	
Data:		
Prev:	0000b9015ce2a08b61216ba5a0778545bf4d	0000ae8bbc96cf89c68be6e10a865cc47c6c4f
Hash:	0000ae8bbc96cf89c68be6e10a865cc47c6c4f	0000e4b9052fd8aae92a8afda42e2ea0f1797e
Mine		

Block:	#	5
Nonce:	56265	
Data:		
Prev:	0000ae8bbc96cf89c68be6e10a865cc47c6c4f	0000e4b9052fd8aae92a8afda42e2ea0f1797e
Hash:	0000e4b9052fd8aae92a8afda42e2ea0f1797e	
Mine		

Subjects ▾

Search



KHAN ACADEMY

< COMPUTER SCIENCE

Journey into cryptography

CONTENTS

About

Ancient cryptography

Ciphers

Cryptography challenge 101

Modern cryptography

Modular arithmetic

Primality test

Randomized algorithms

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

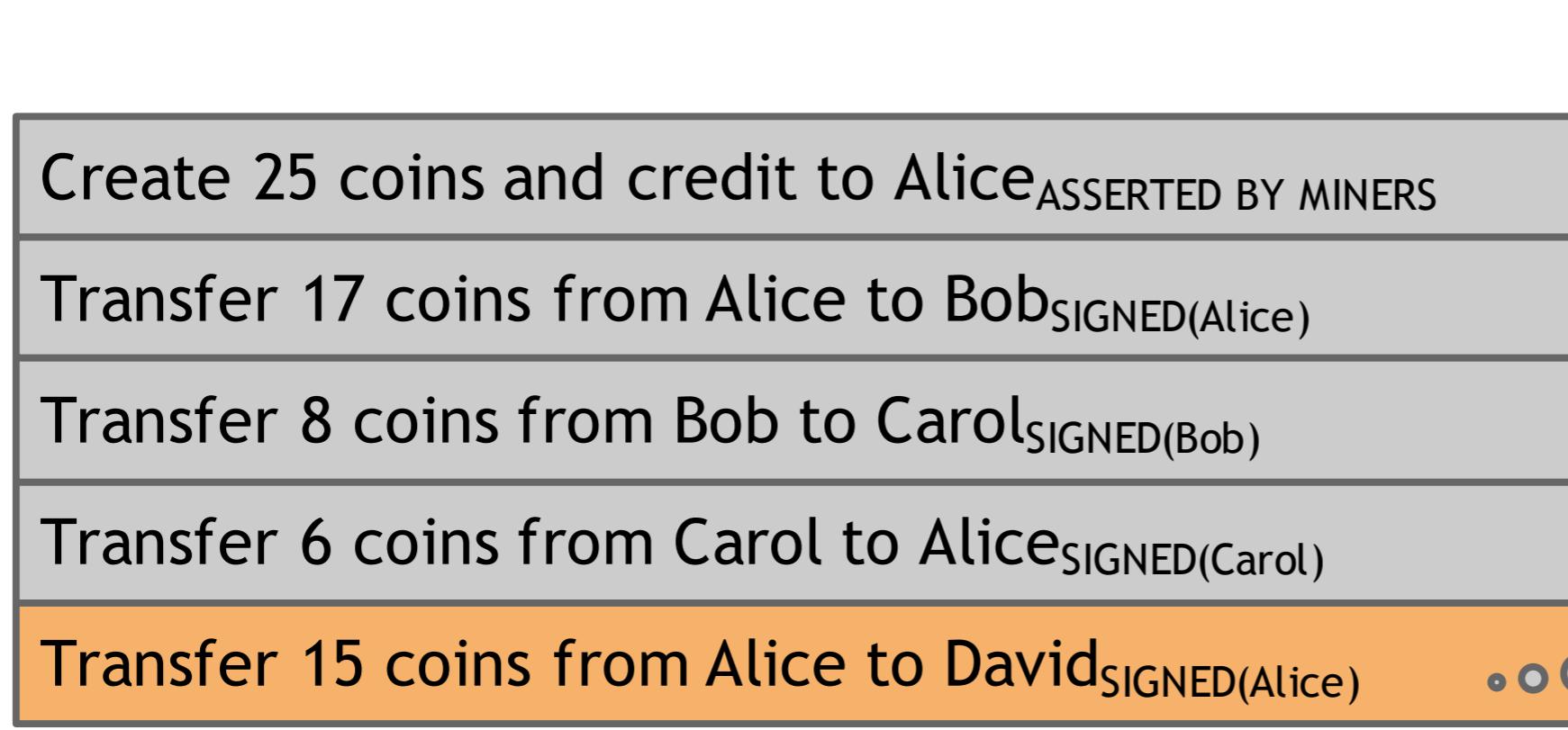
上次没讲完部分

交

易

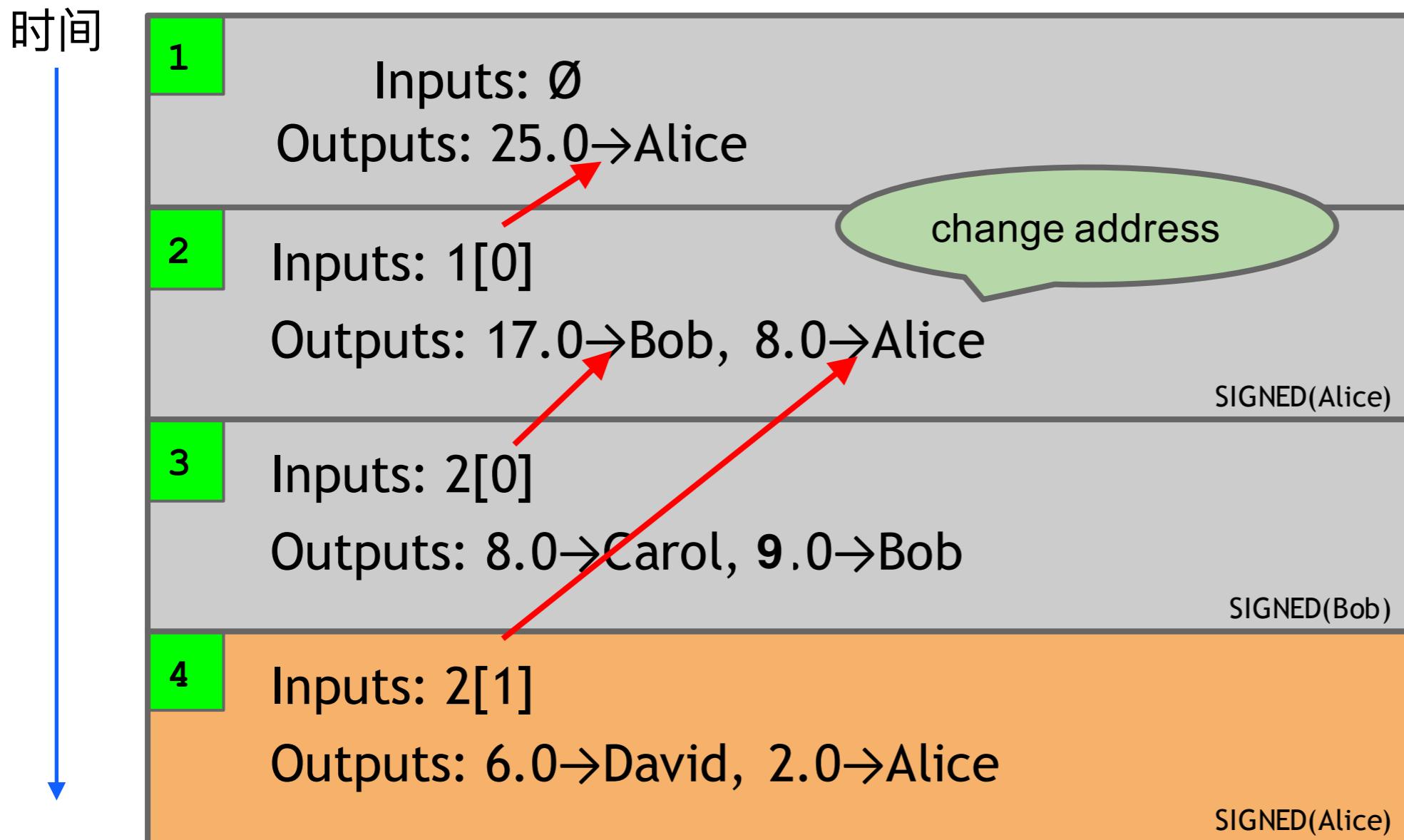
普通账本

时间



一个块包含一个交易

交易验证需要扫描以前所有的块

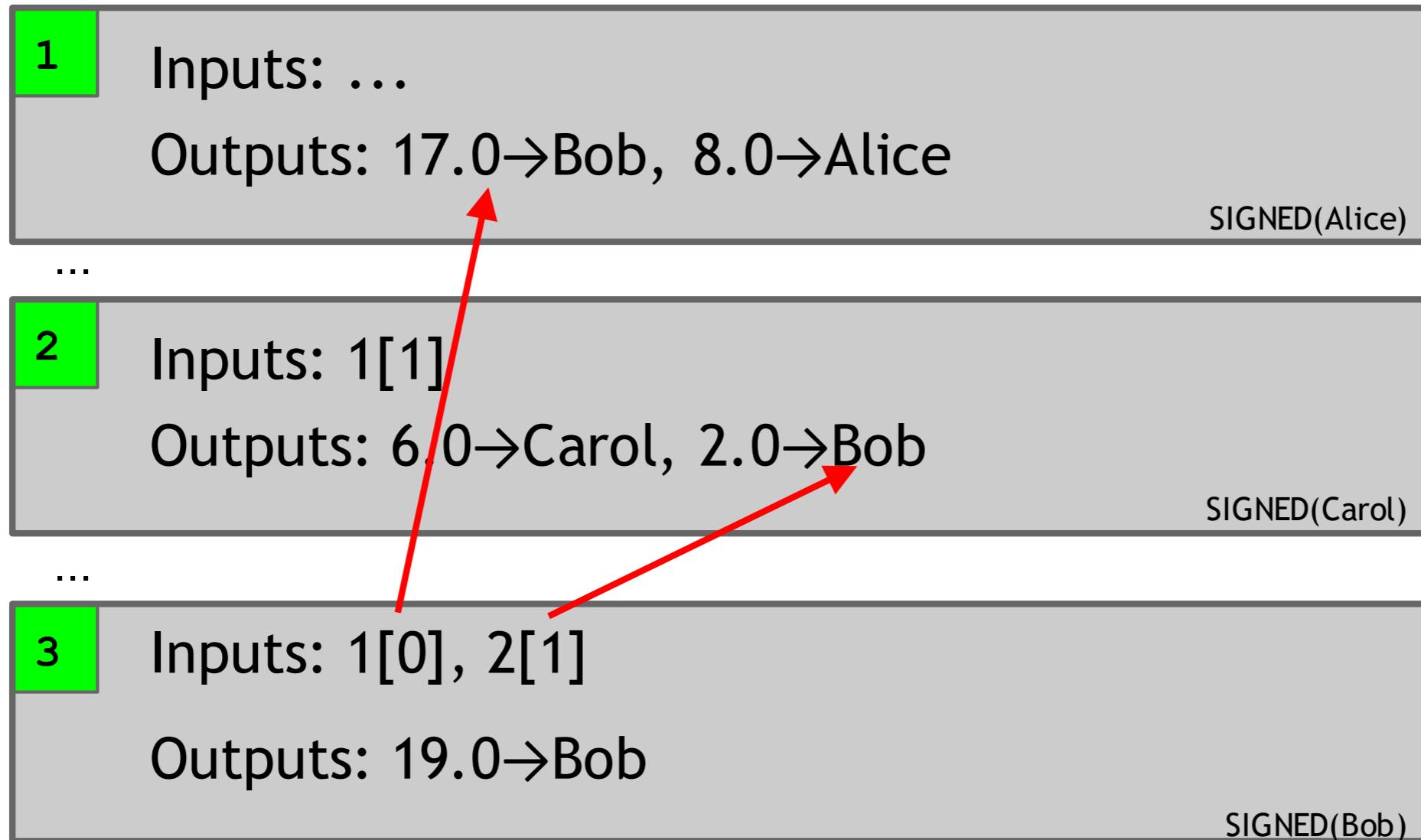


一个块包含一个交易

交易验证需要扫描以前所有的相关块

合并

时间

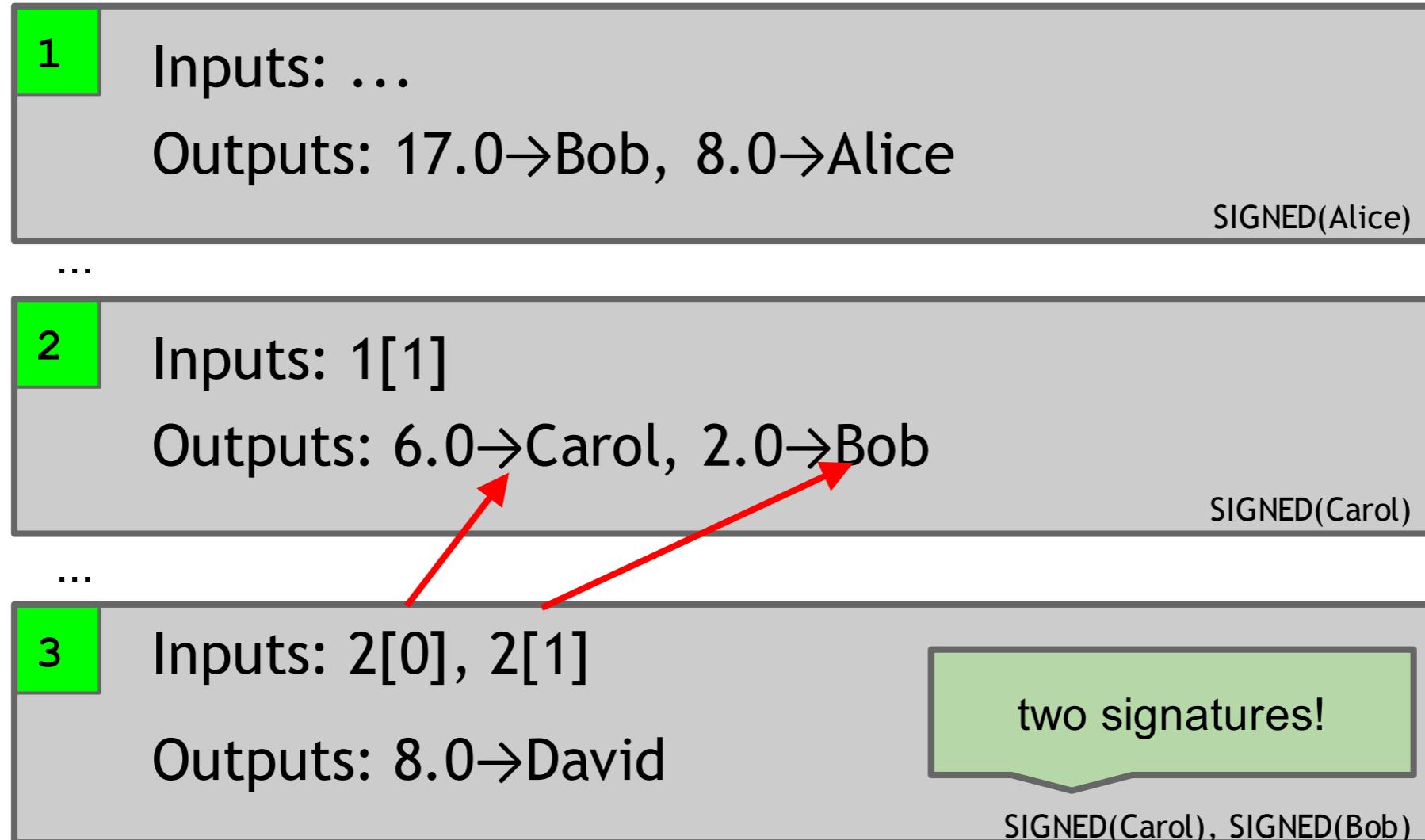


一个块包含一个交易

交易验证需要扫描以前所有的相关块

联合支付

时间



一个块包含一个交易

脚本

比特币交易

```
{  
    "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"  
        }  
    ]  
}
```

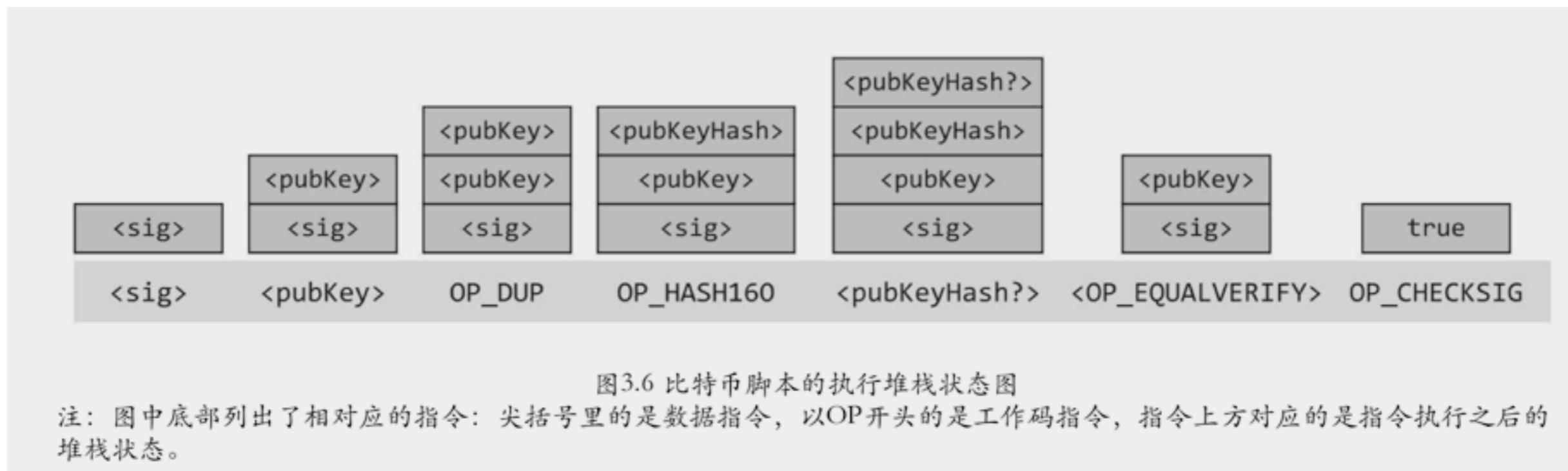
图3.3 一个真实的比特币交易程序段

比特币脚本

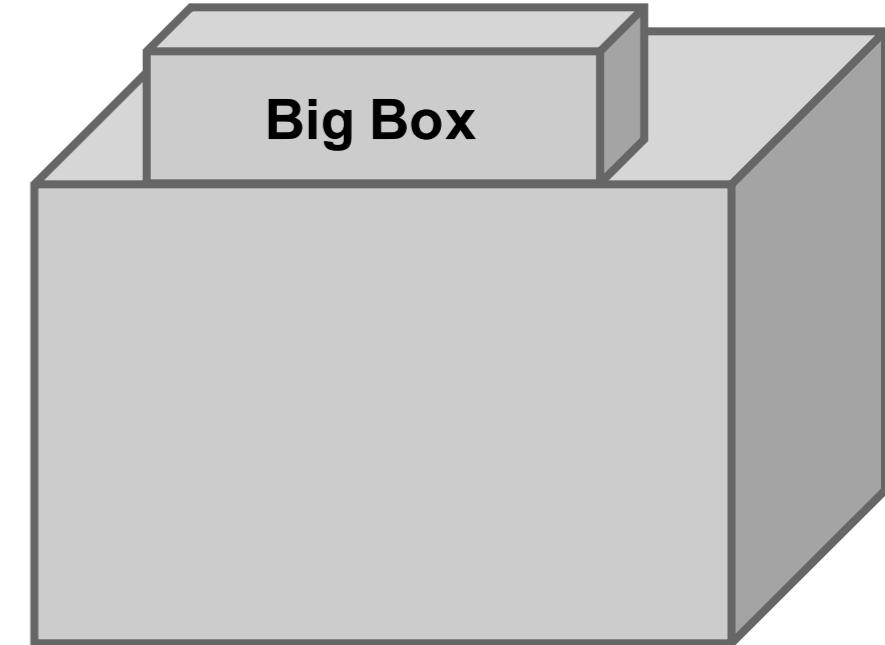
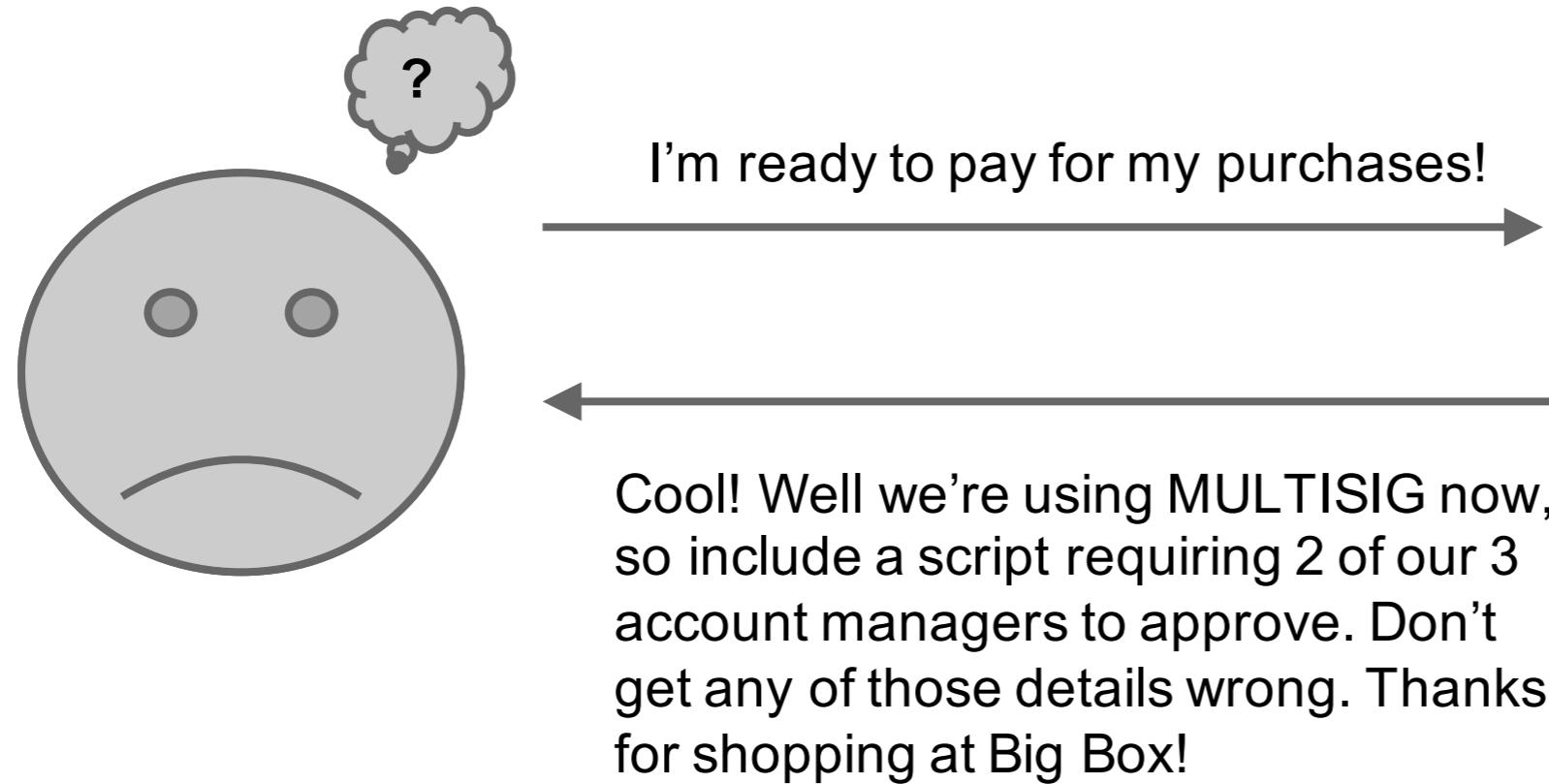
```
OP_DUP  
OP_HASH160  
69e02e18...  
OP_EQUALVERIFY  
OP_CHECKSIG
```

图3.4 P2PH脚本范例

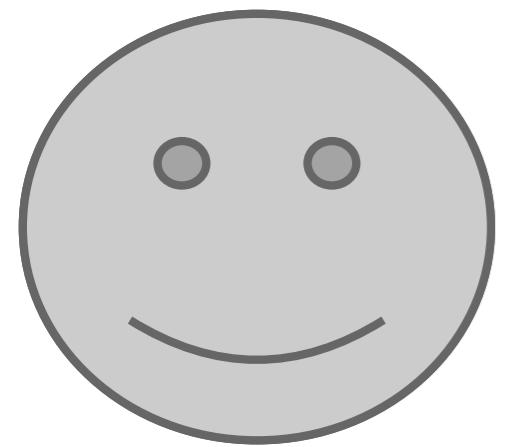
```
<sig>  
<pubKey>  
-----  
OP_DUP  
OP_HASH160  
<pubKeyHash?>  
OP_EQUALVERIFY  
OP_CHECKSIG
```



多重签名问题

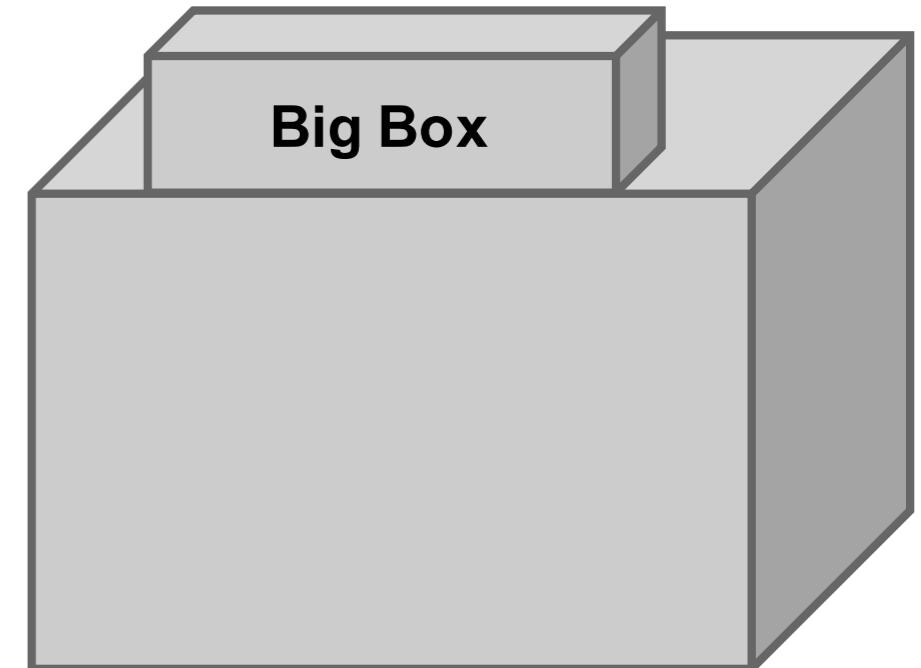


Pay for Script

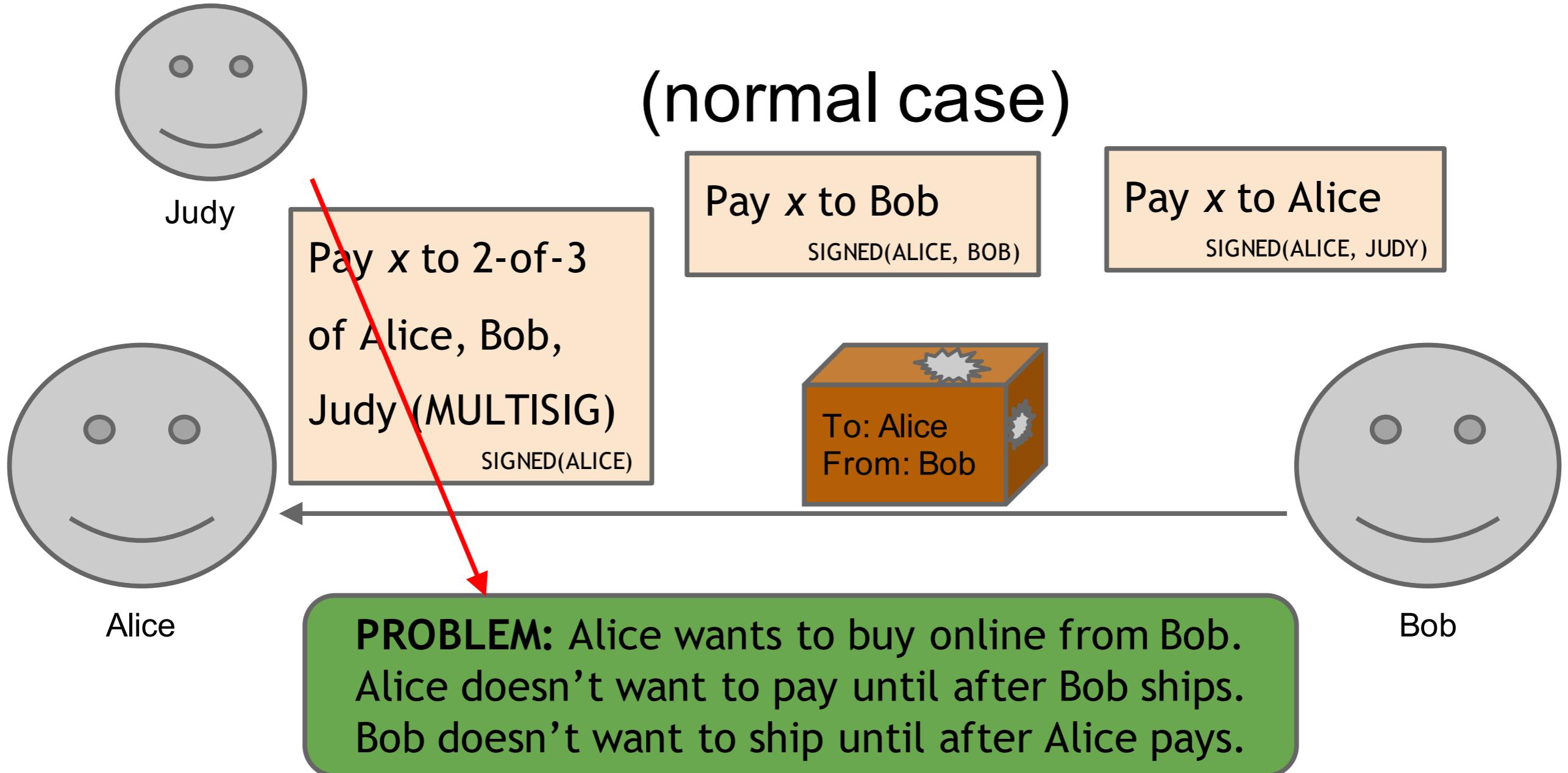


I'm ready to pay for my purchases!

Great! Here's our address: 0x3454

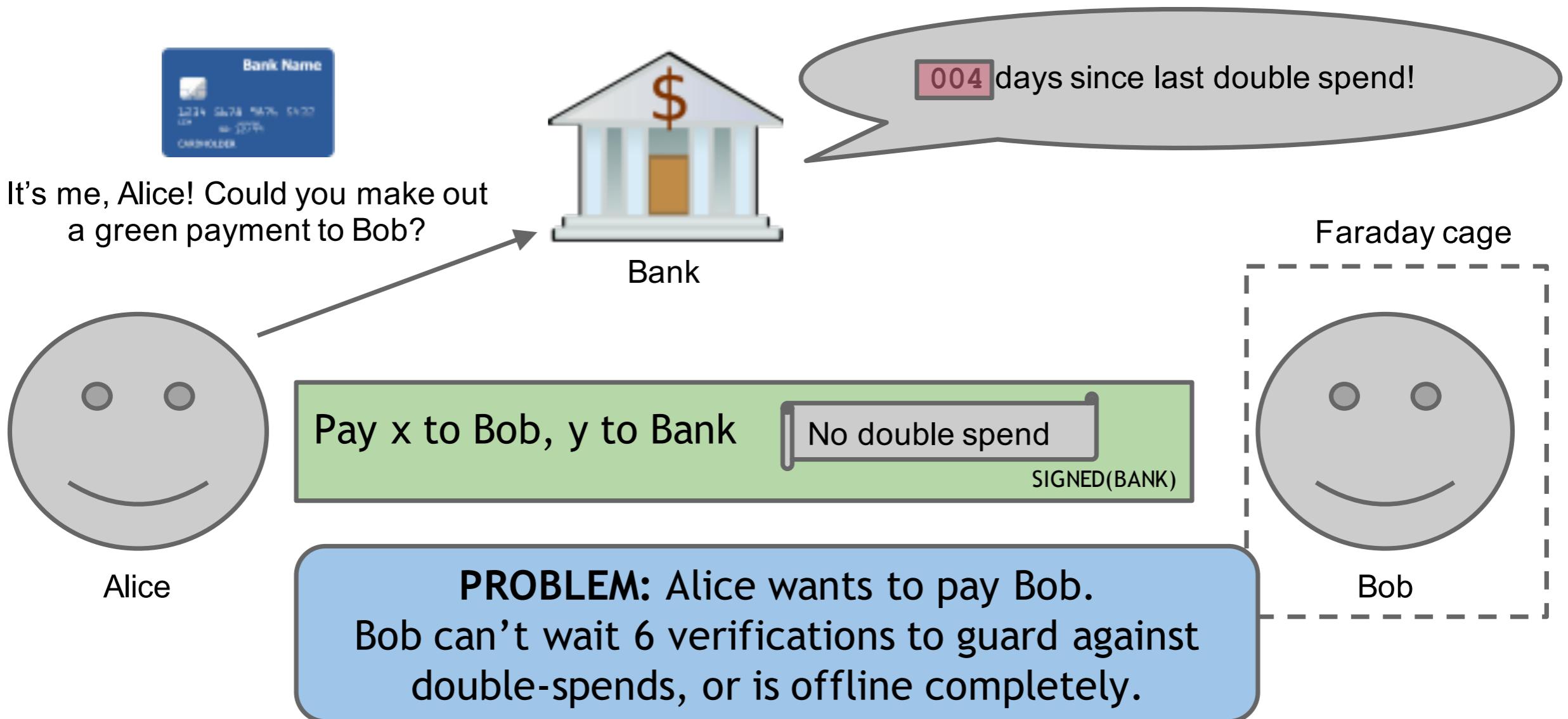


托管

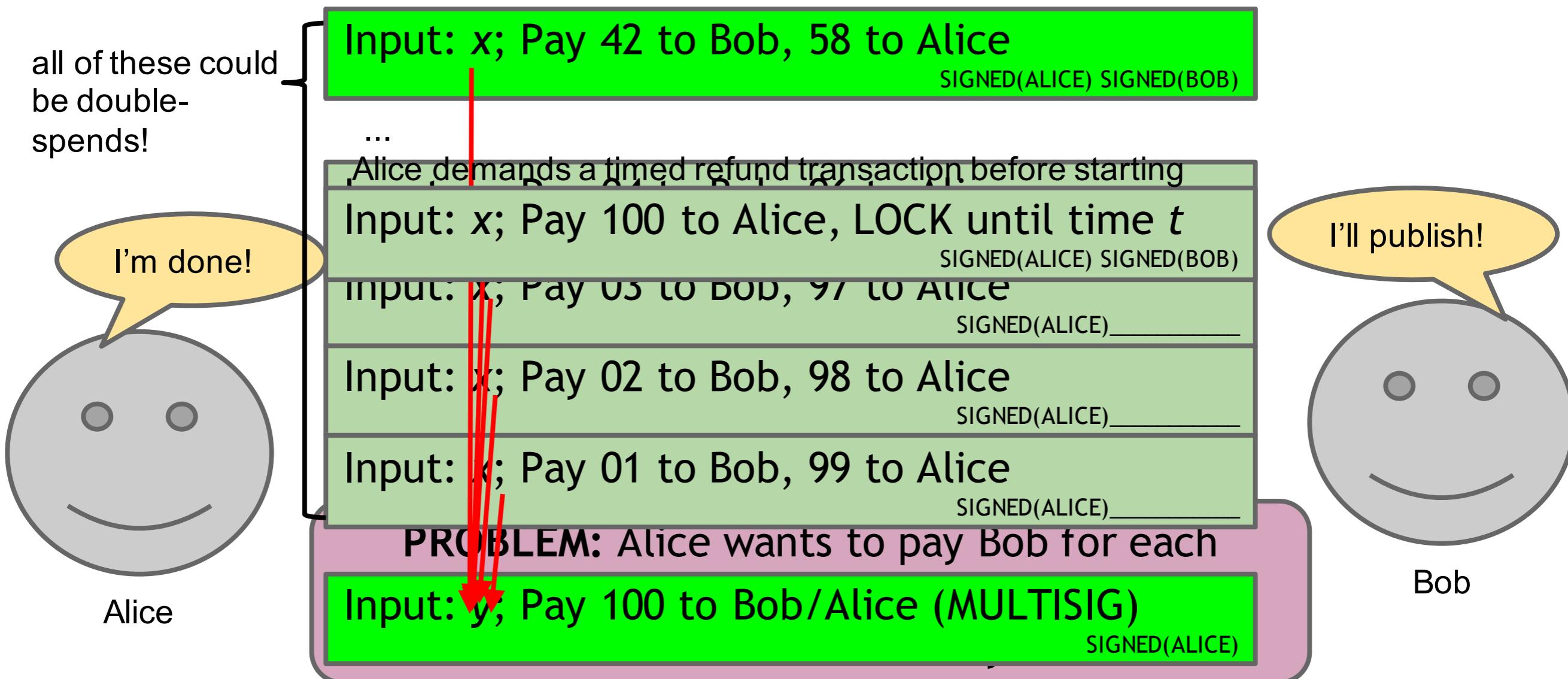


Blockchain Technology

绿色地址



小额多次交易



锁定时间

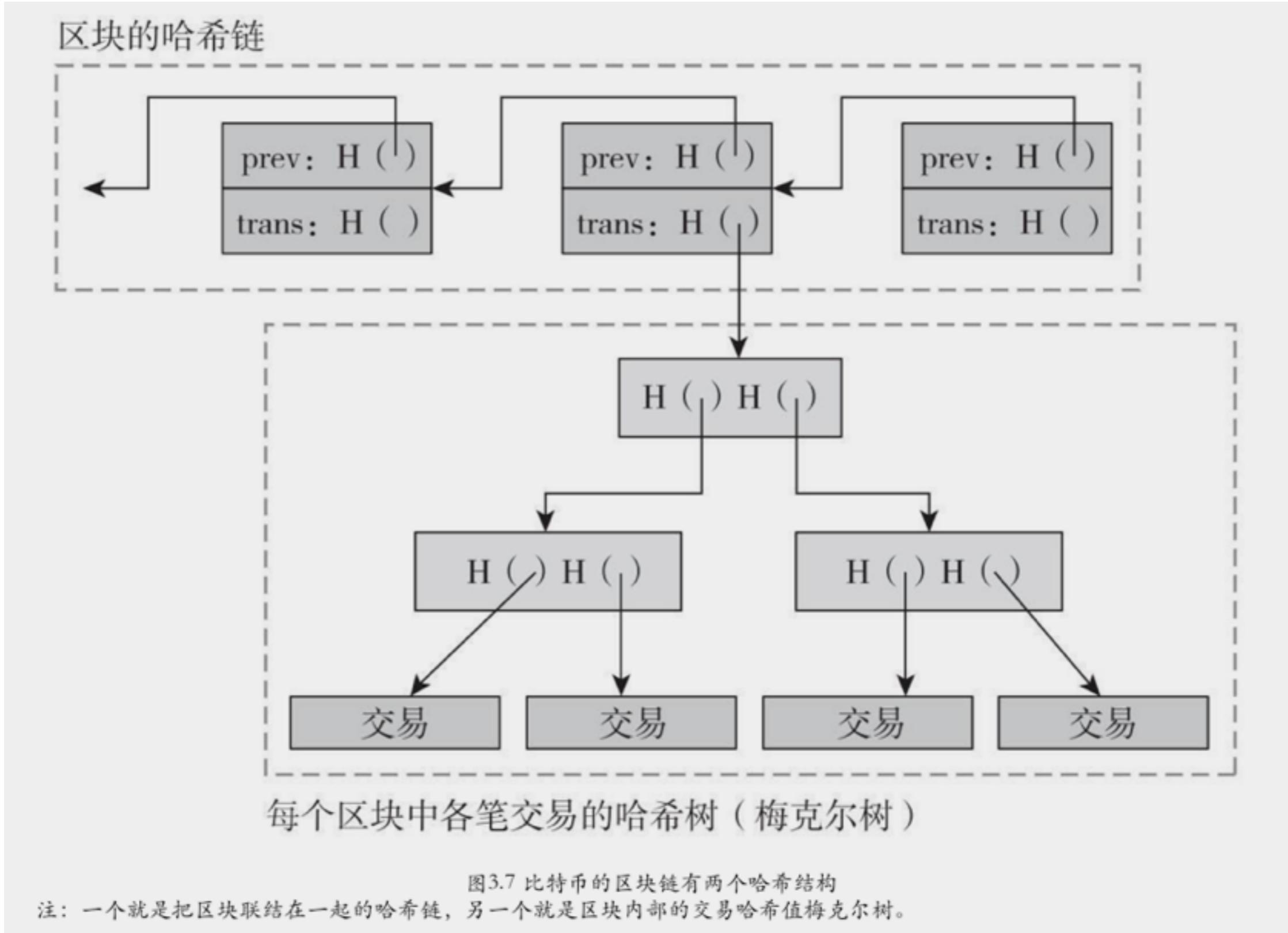
```
{  
  "hash": "5a42590...b8b6b",  
  "ver": 1,  
  "vin_sz": 2,  
  "vout_sz": 1,  
  "lock_time": 315415,  
  "size": 404,  
  ...  
}
```

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

区

块

比特币的区块结构



币基交易

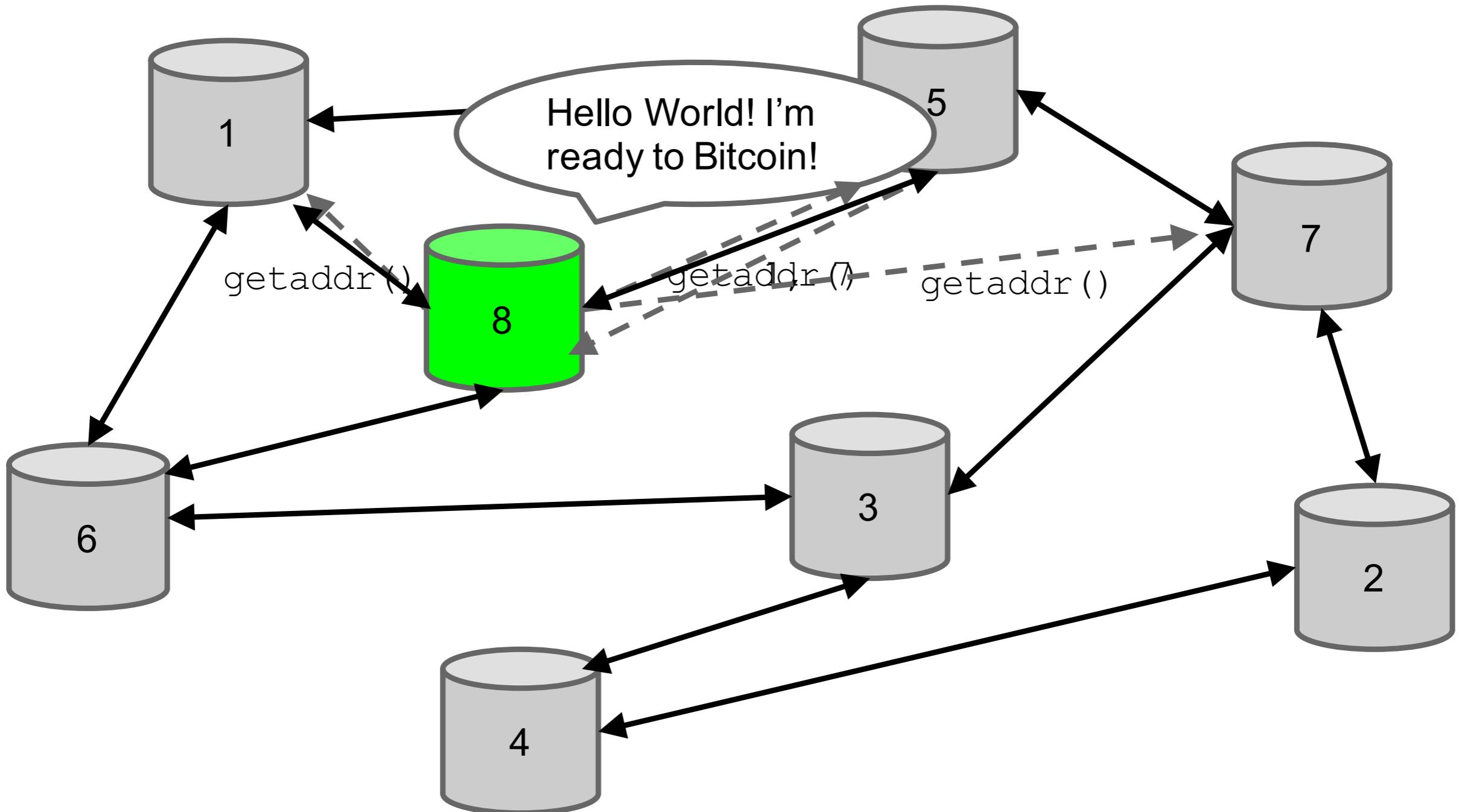
```
"in": [
    {
        "prev_out": {
            "hash": "000000....000000",
            "n": 4294967295
        },
        "coinbase": "..."
    },
    [
        ...
    ]
],
"out": [
    {
        "value": "25.03371419",
        "scriptPubKey": "OPDUP OPHASH160 ... "
    }
]
```

图3.8 币基交易

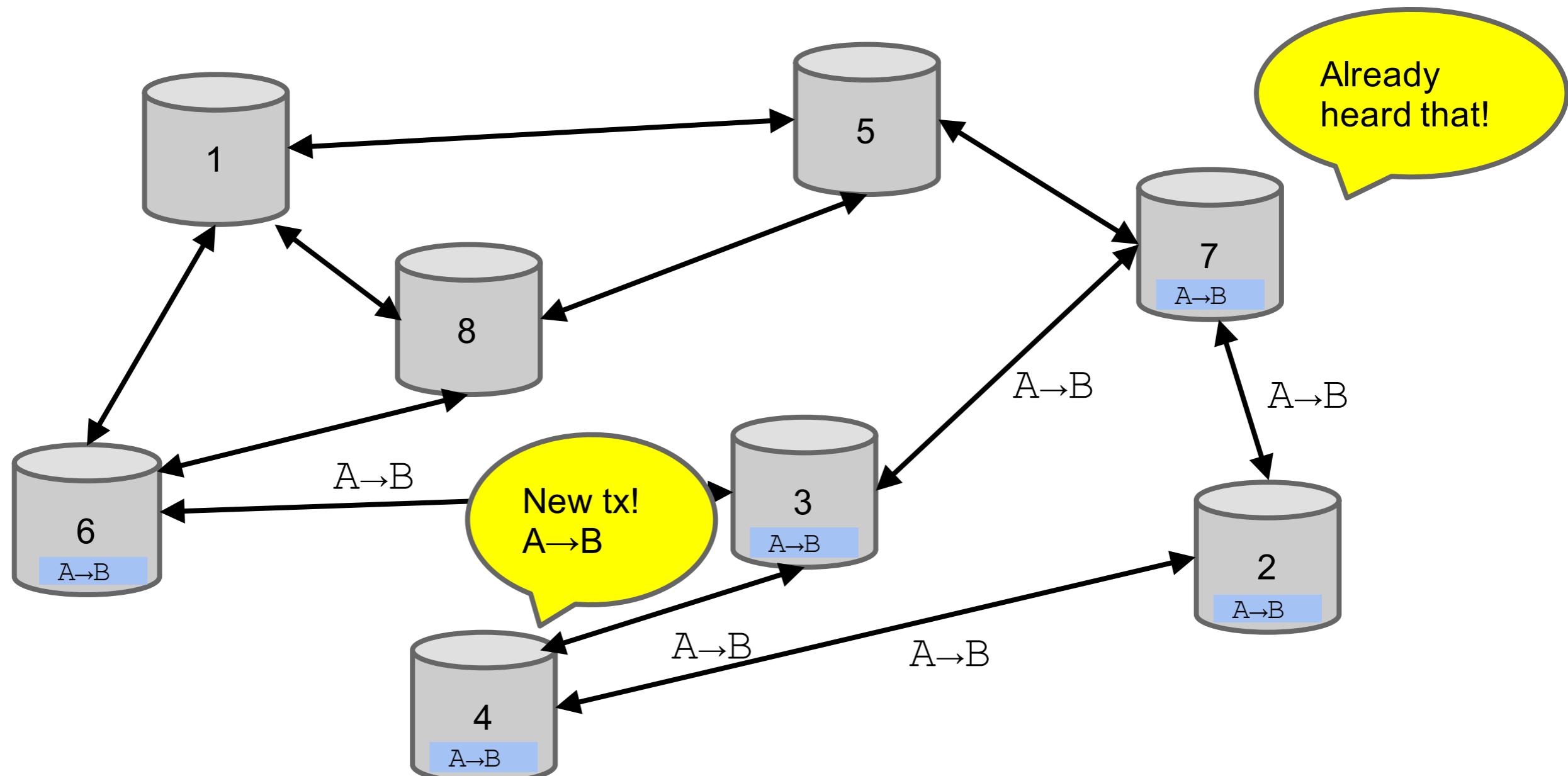
网

络

比特币网络



比特币网络交易消息传播



块传播

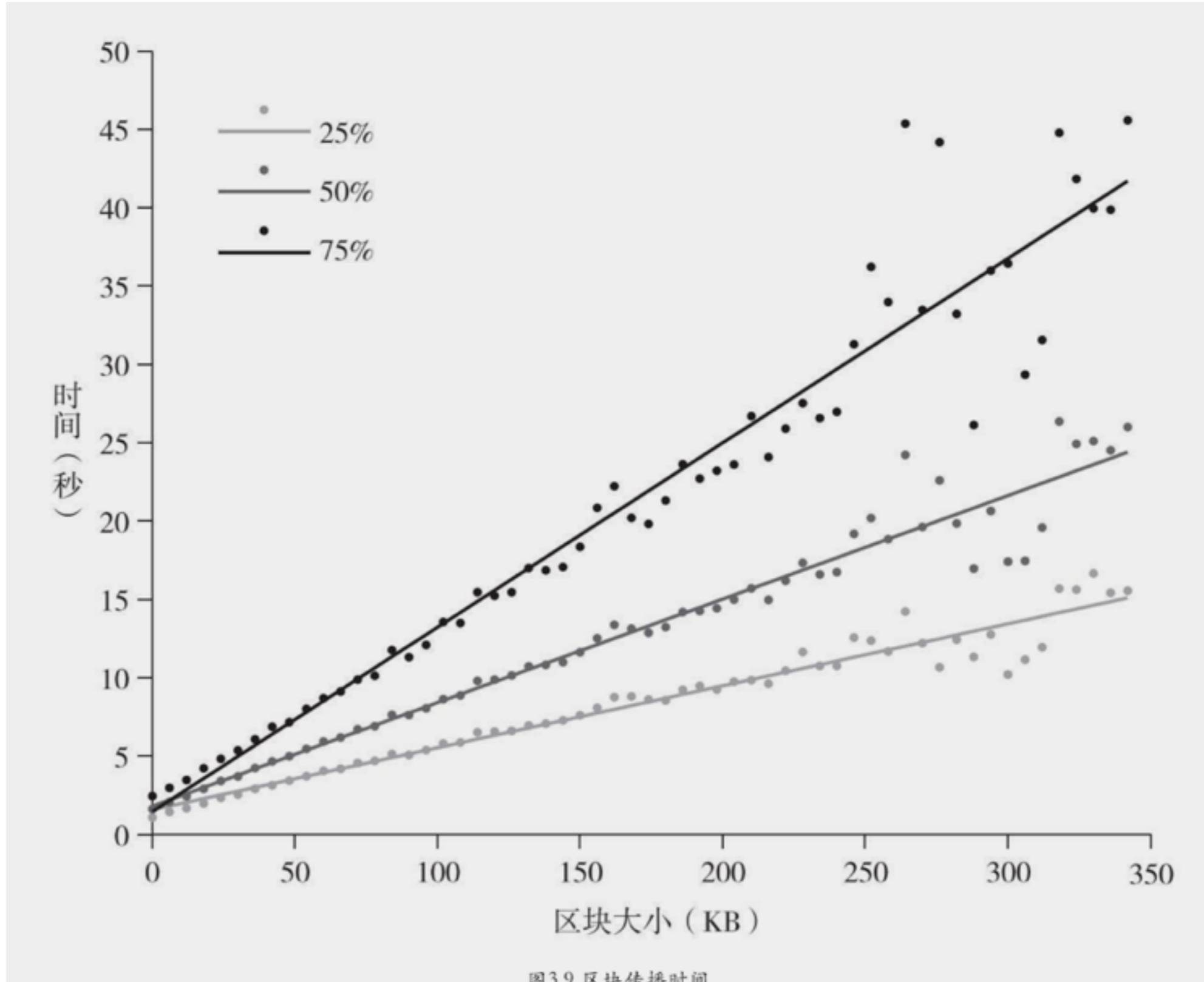
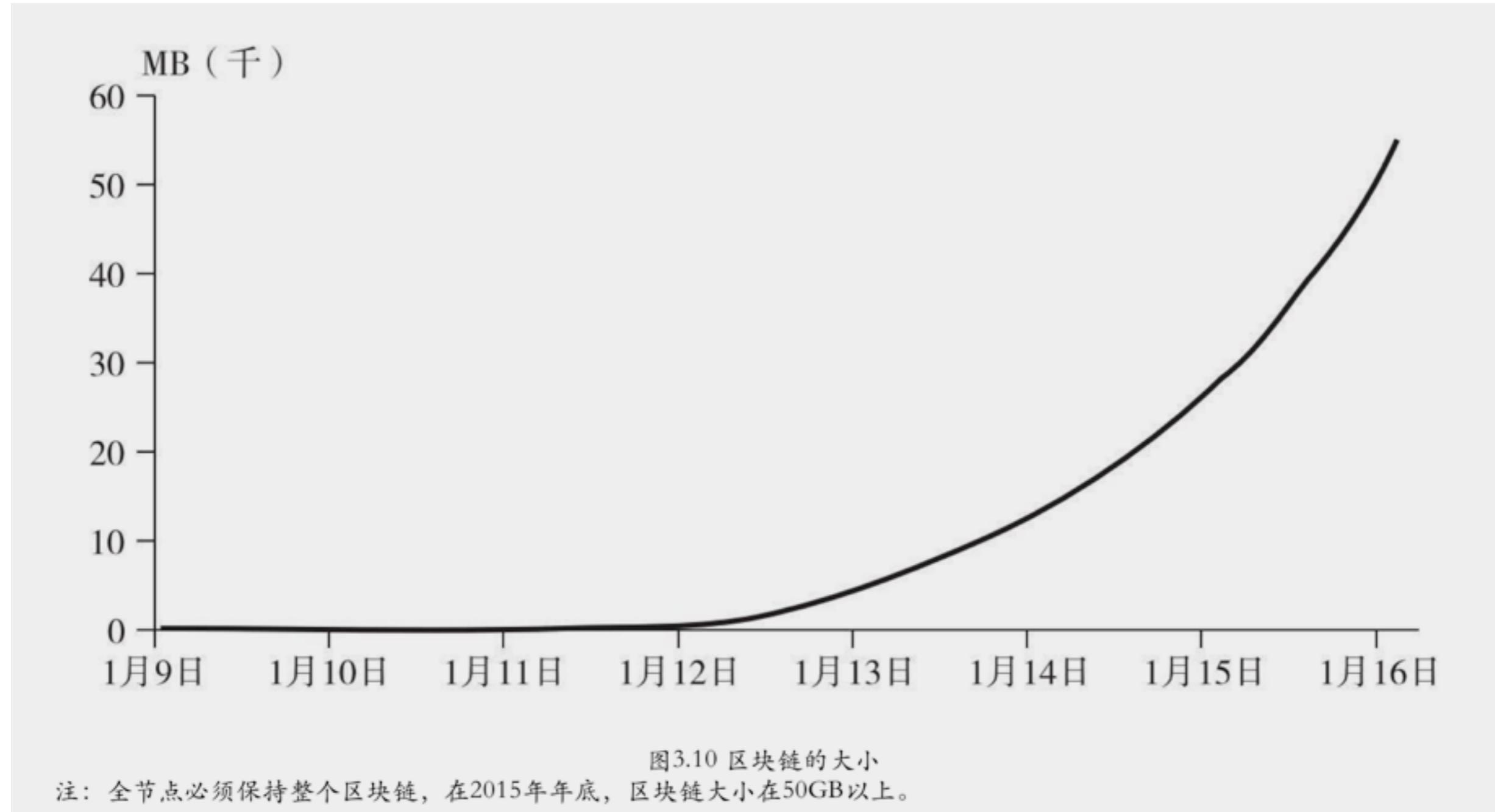


图 3.9 反映传播时间

存储花费



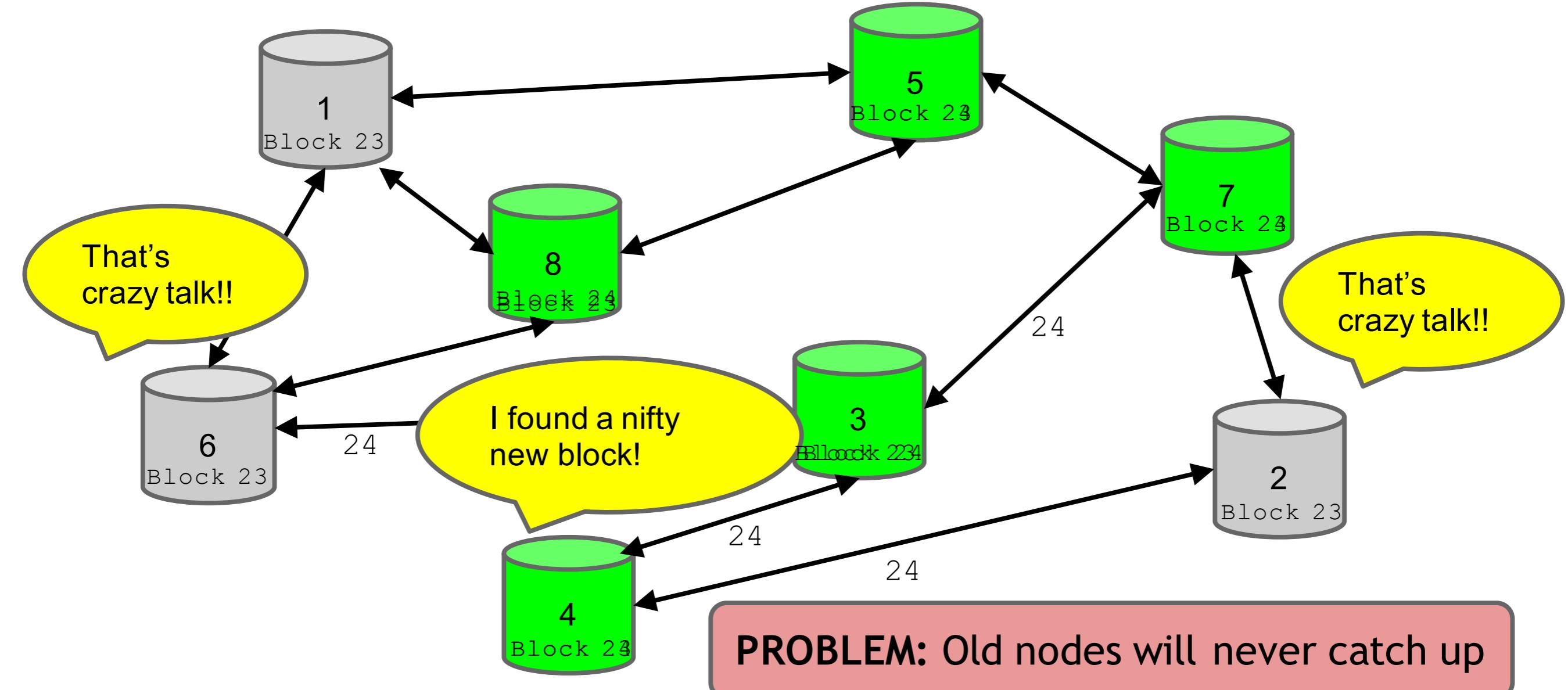
限制

比特币限制

- 10分钟：产生块的间隔
- 1M：一个快大小
- 2万签名：每个快
- 100M *satoshi*：每个币
- 23M：比特币再大
- 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)

Blockchain Technology

分叉



硬 vs. 软

存 儲

比特币存储

Hot storage



online

Cold storage



offline

hot secret key(s)

payments

cold address(es)

Blockchain Technology

威胁



Charles Ponzi



Blockchain Technology

交易所



提问时间！

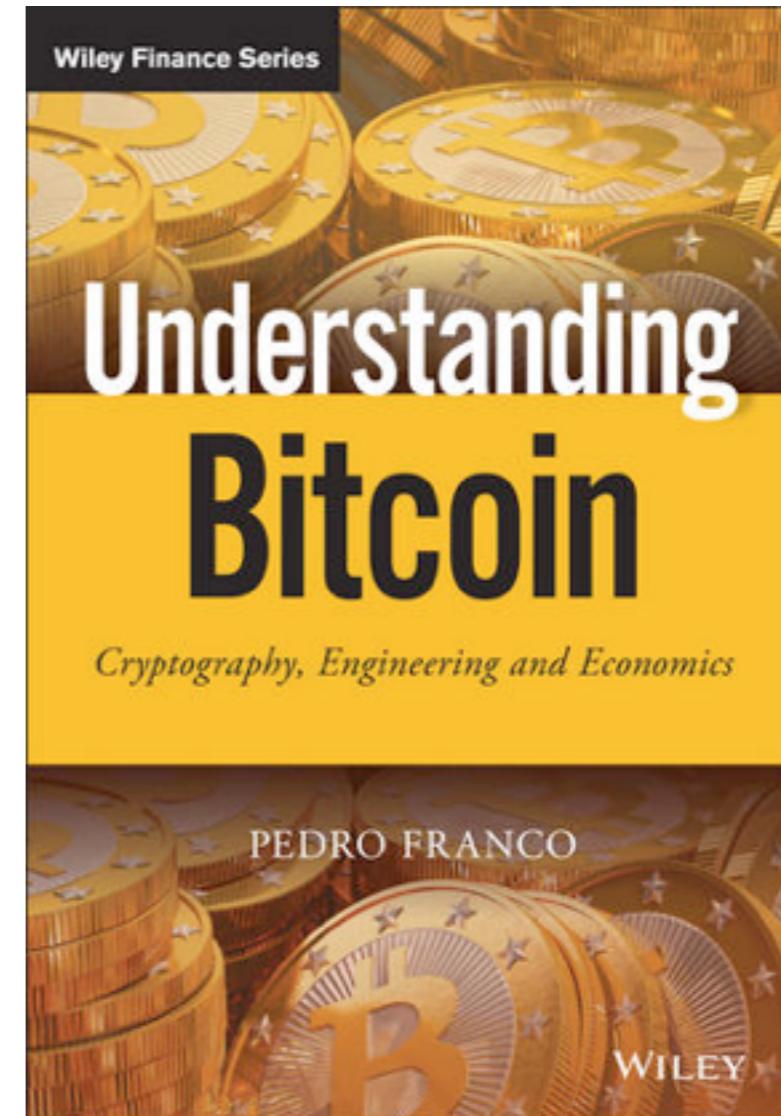
Home work

Homework

课后作业



第三章、第四章



第六章、第八章

- 要求阅读如下论文，写论文阅读报告：

→ *In IEEE Computer Magazine 2017.*

COVER FEATURE BLOCKCHAIN TECHNOLOGY IN FINANCE



谢谢！

孙惠平

sunhp@ss.pku.edu.cn