EDU

CSDN学院　IT实战派

比特币定位和区块链原理

比特币的定位和原理

讲师：　康烁

课程目标

1. 了解区块链、智能合约原理
2. 理解以太坊原理
3. 掌握DApp开发工具
4. 运用Solidity开发智能合约
5. 掌握DApp开发逻辑与技术

本章目标

1. 理解比特币和区块链的原理
2. 理解双花和解决方案
3. 理解数字货币发行和挖矿

本节目标

1. 了解比特币的本质
2. 理解比特币的交易不可篡改和复制的技术手段 

3. 理解中心化系统的数字支付存在的问题

一切都从比特币是数字现金谈起

Bitcoin: A Peer-to-Peer Electronic Cash System

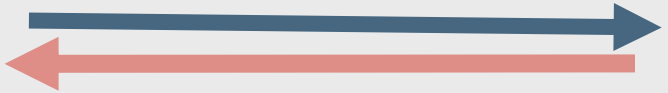
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third 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 hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace 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.

现金最大的作用

立即可以投入流通的交换媒介

流通，支付



现金的一些特性

- 可以验证，不可伪造
- 现金不可复制（物理特性）
- 支付流程

这样一个过程可以被称为是一次交易

现金的直接数字化

- 支付宝
- 微信支付
- 信用卡
- 银行卡

如何保证可以验证？不可伪造？不可复制？

有啥不爽的?

- 是中心化的系统
- 中心化，中心化的人
  - 1）可以干坏事
  - 2）只能信任他?
  - 3）银行知道所有信息
- 如果我们不相信任何人
  - 直接点对点的数字现金

直接的点对点的数字现金——比特币

- 比特币!
- 所有人都不互相信任
- 可以直接点对点支付
- 具有现金的特征

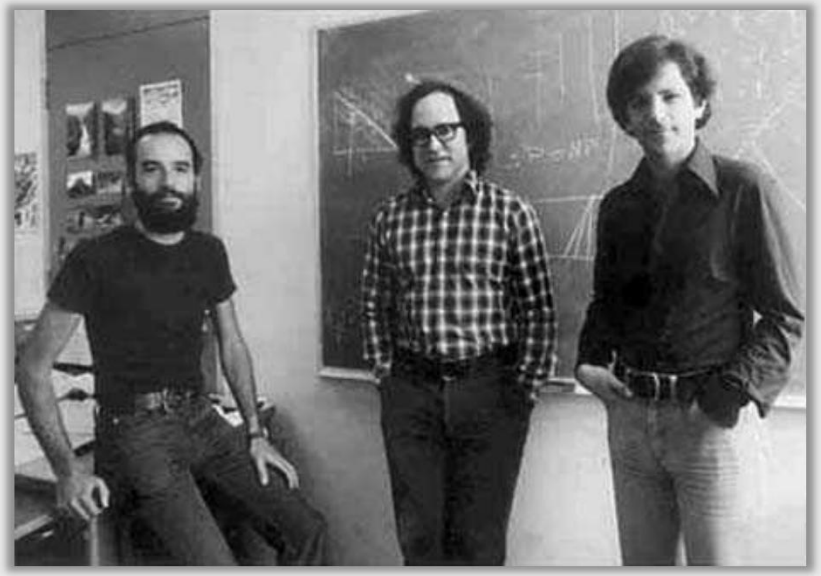
思考一下？数字货币需要解决什么问题

- 现金的发行问题
  - 不能依赖于外部发行
- 现金的支付流程问题
  - 不可抵赖
  - 不可篡改
  - 不可双花

现金最终要的功能：支付

- 支付最终要的是：验证现金的真假，包括数字现金
- 纸币通过水印的办法保证不可伪造
- 数字现金怎么办？

数字签名



Rivest, Shamir, Adleman

签名的特性

不可伪造

不可抵赖

数字签名

- 不可抵赖
- 不可伪造

- 非对称加密算法：每个人有一个私钥，有一个公钥
- 公钥是公开的，私钥是秘密的
- 私钥用来签名，公钥用来验证

数字货币的交易

不可伪造

不可抵赖

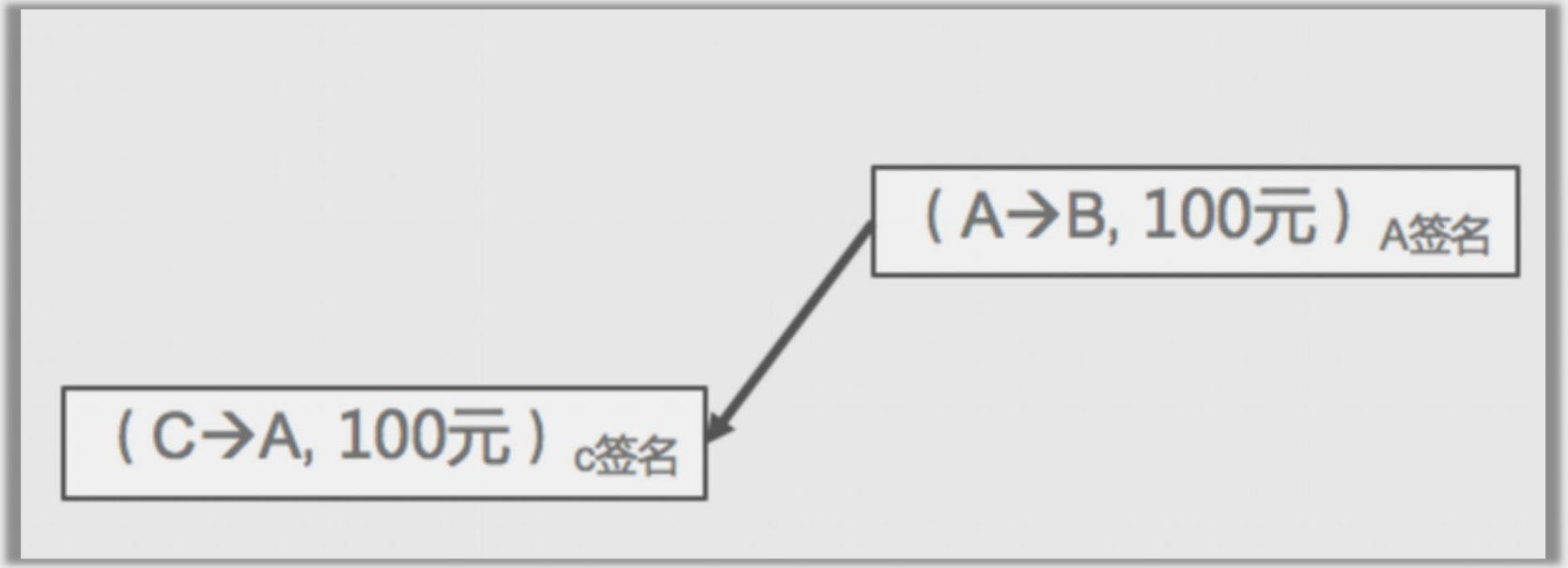
是否就代表了一次合法的交易?

（A→B, 100元） A签名

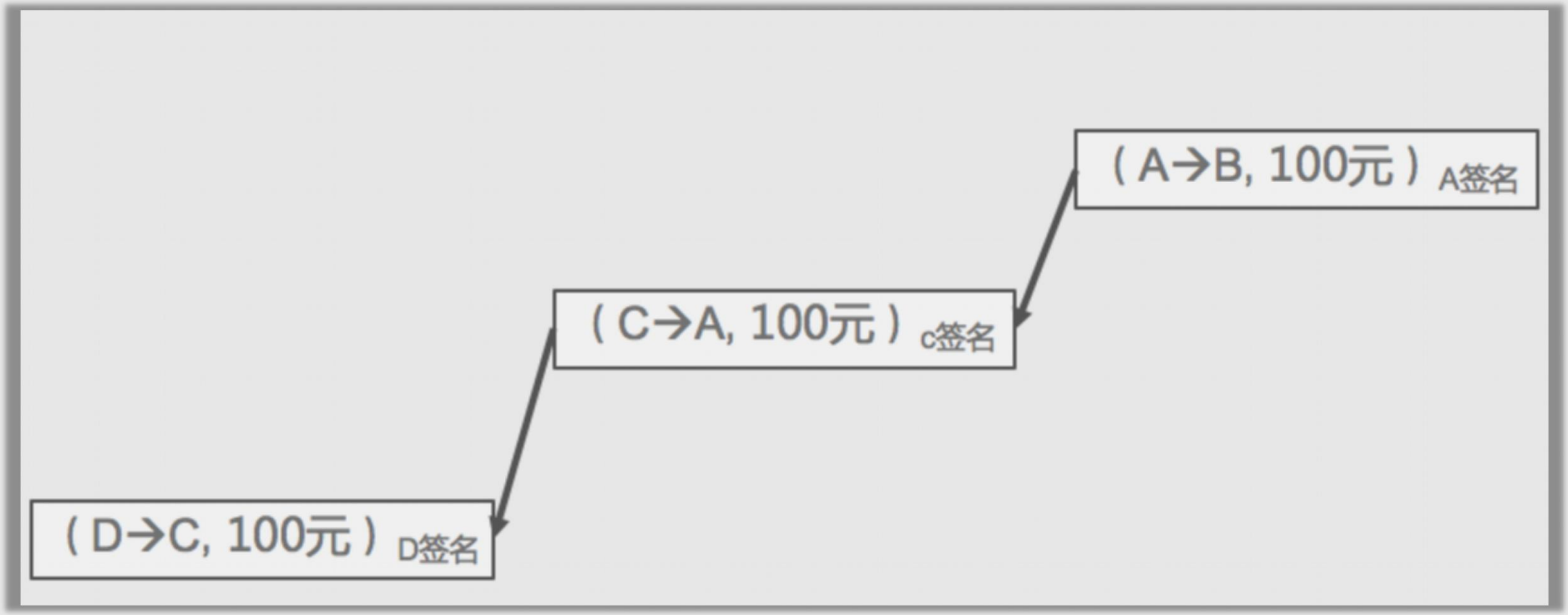
1. 需要证明A获得的100元是合法的来源
2. 需要证明A没有把同样的钱花两次

（A→A, 100元） A签名

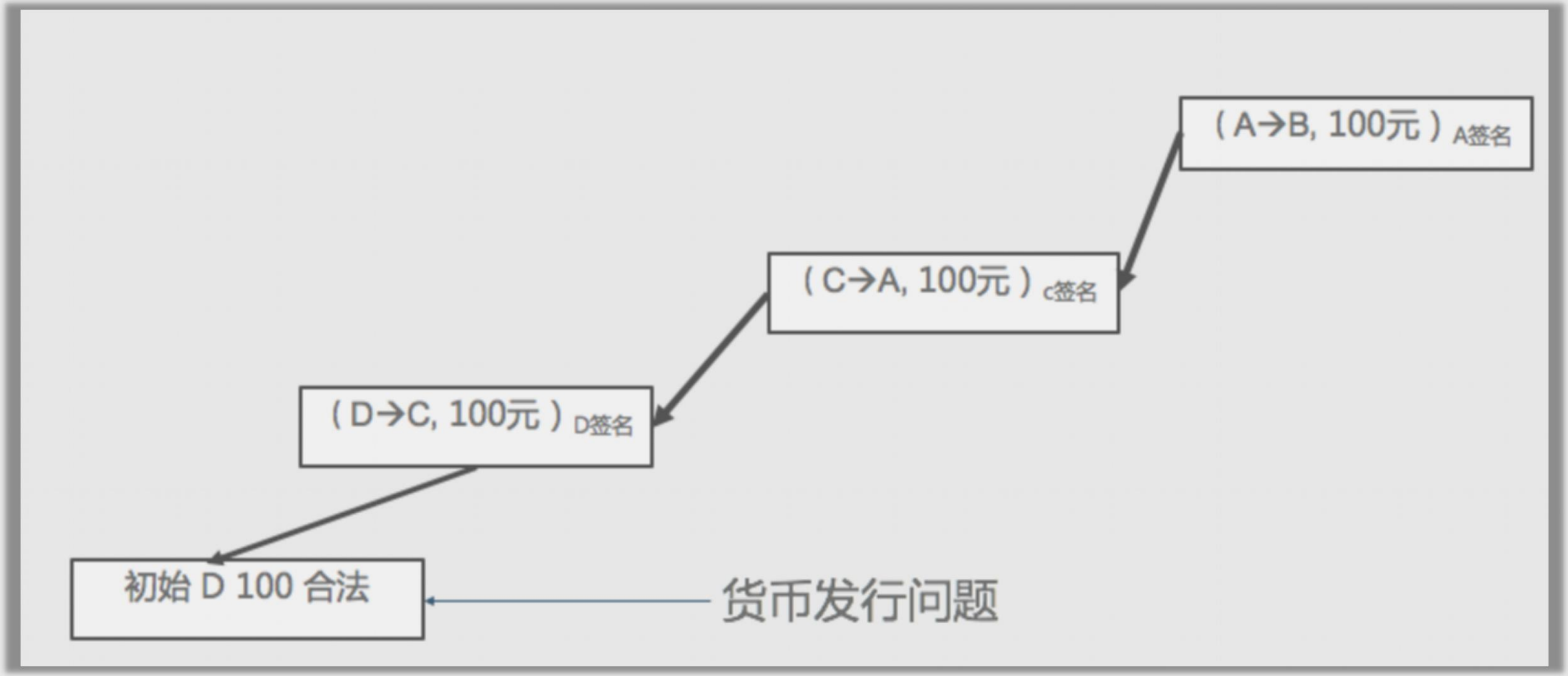
合法来源的问题



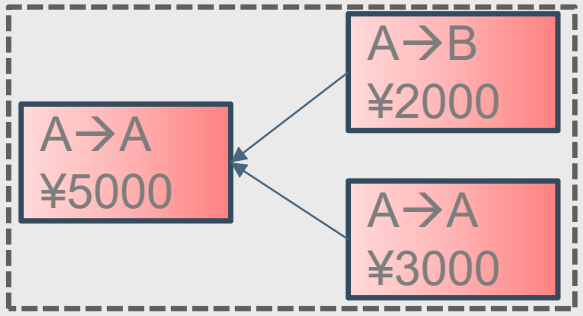
合法来源问题

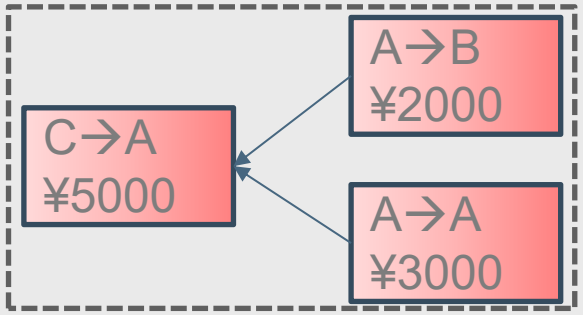


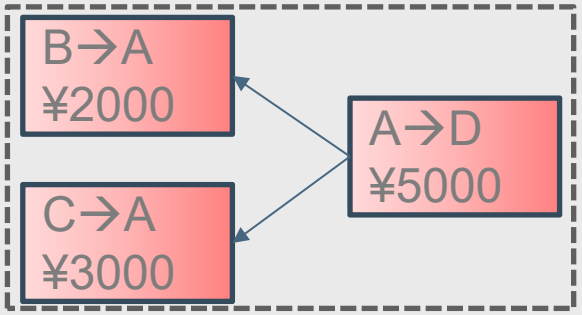
合法来源问题

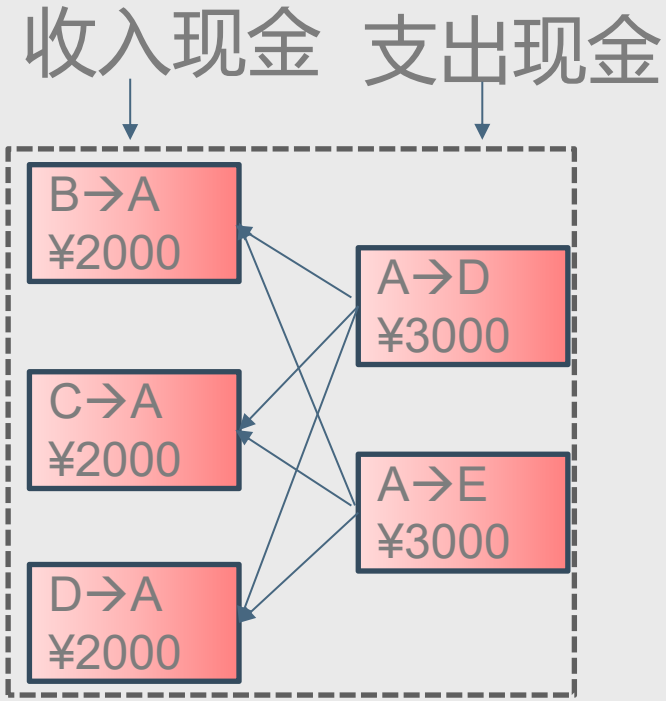


交易就是现金!









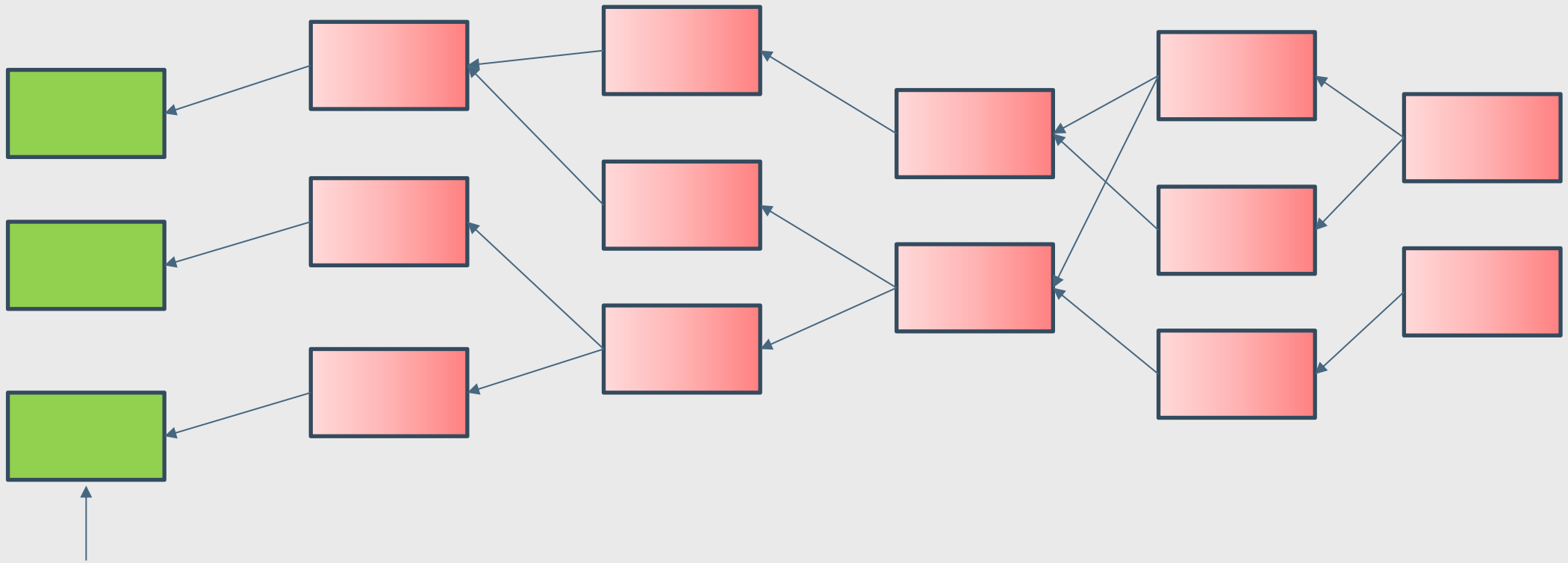
跟实物现金一样，数字现金也是能被花出去，且只能被花出去一次

一次流通

如何判断是不是真的钱?

- 来源是合法的，最终由一个合法的发行方法来定义!
- 溯源的链上每一笔交易都是合法的，所有的交易（现金）都可以验证
- 每一次流通的收入现金之和等于支出现金之和

这样，我们就有一个交易的网络，也就是现金的网络



你得需要保证一开始的钱是真的

小结

1. 比特币本质是点对点的数字现金系统
2. 数字签名可以防篡改和伪造交易

布置作业

- 必做内容
- 阅读比特币白皮书，了解比特币的起源和设计思路

EDU

CSDN学院　IT实战派