EDU

CSDN学院　IT实战派

比特币定位和区块链原理

比特币的双花和区块链

讲师：康烁

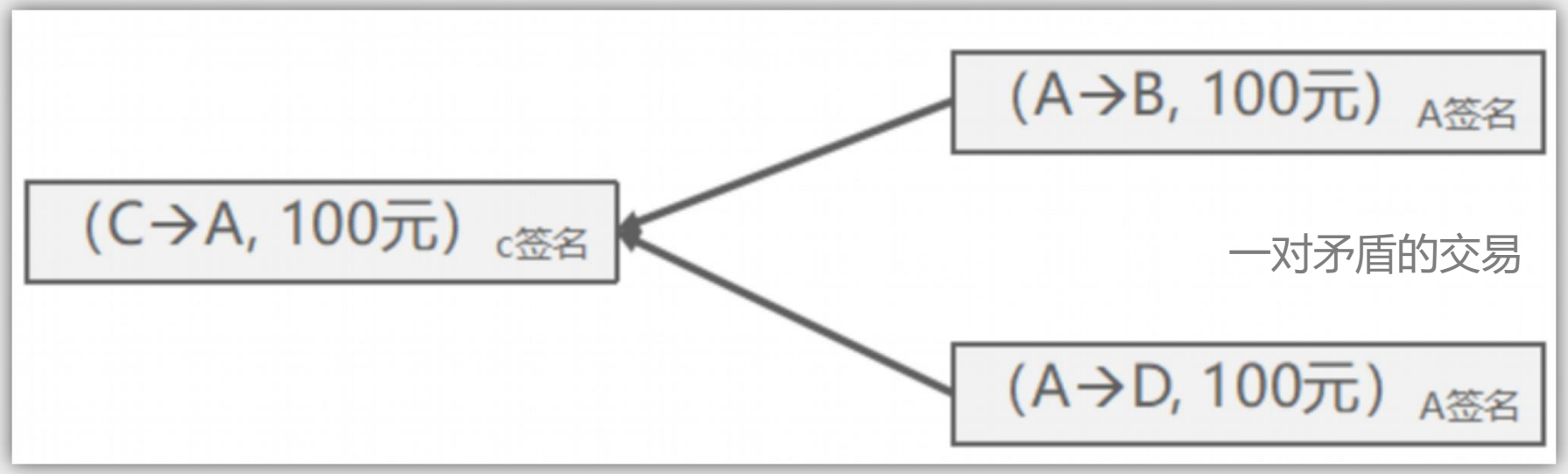
本节目标

1. 了解为什么存在双花问题
2. 理解双花问题的基本原理
3. 掌握一句话解释区块链的能力

货币的双花（复制）为啥会成为问题?

实物现金不会出现双花的问题

中央机构的数字货币也不会



1. 这件事情对A来说很简单
2. A告诉一部分人一个交易，另外一部分人另外一个交易
3. 分别看起来这两个交易都是合法的
4. 合起来看就不对了

如何达到阻止双花的目的?

1. 支付过程全网广播，所有人都可见，所有人都看到相同的交易
2. 需要一种表达形式来达到这个目标

坏人能做什么？

1. 一个矛盾的交易
2. 给一部分人这个交易
3. 给另外一部分人那个交易
4. 出现了double spending（双花，复制）

如何不让坏人干坏事?

1. 不要相信发出的交易，直到确认
2. 把坏人变成好人

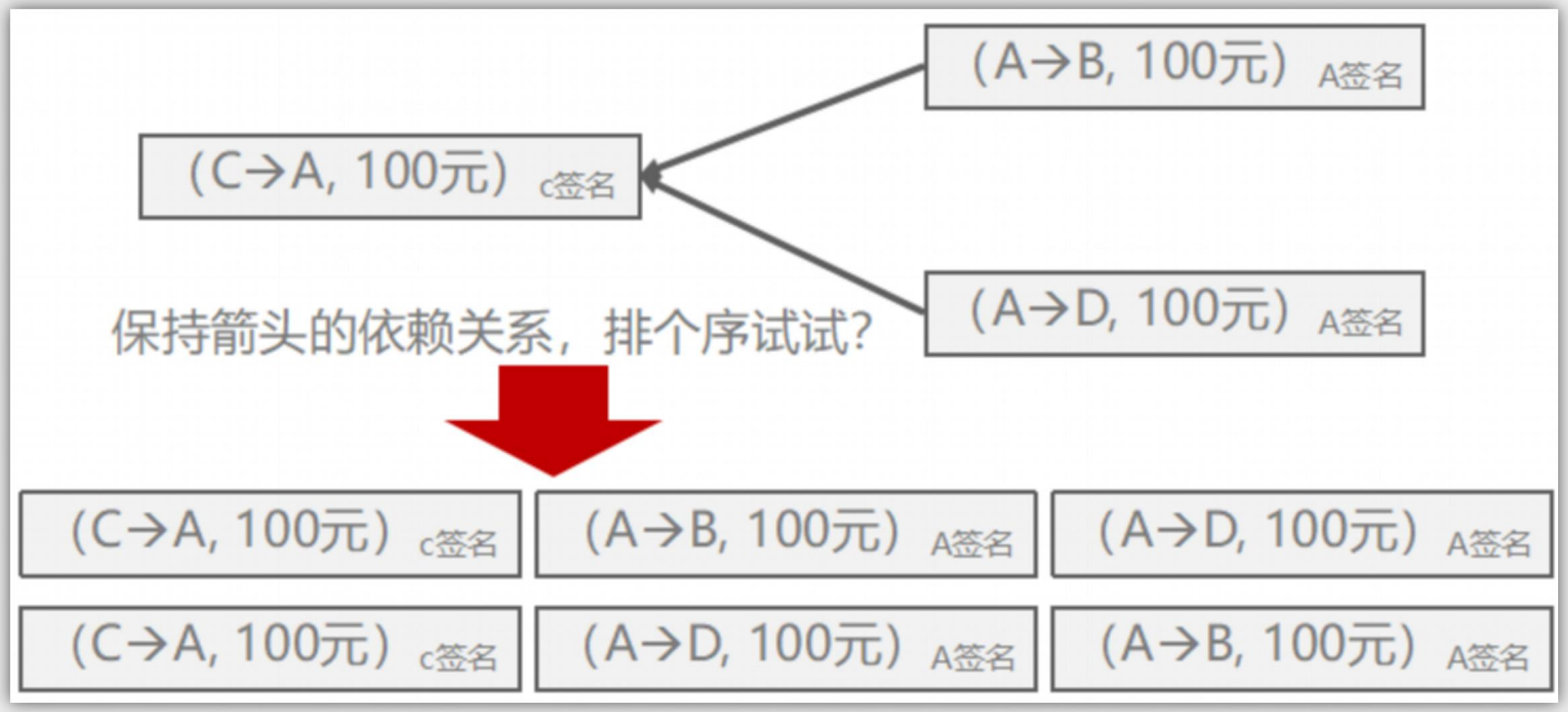
如何确认交易？

大部分人同意一个交易（少部分同意不行，交易有非确认的交易，有确认的交易）

如何把坏人变成好人

1. 比特币的伟大发明：破坏系统需要投资大但是获益不大，支持系统获益大
2. 手段：通过激励机制

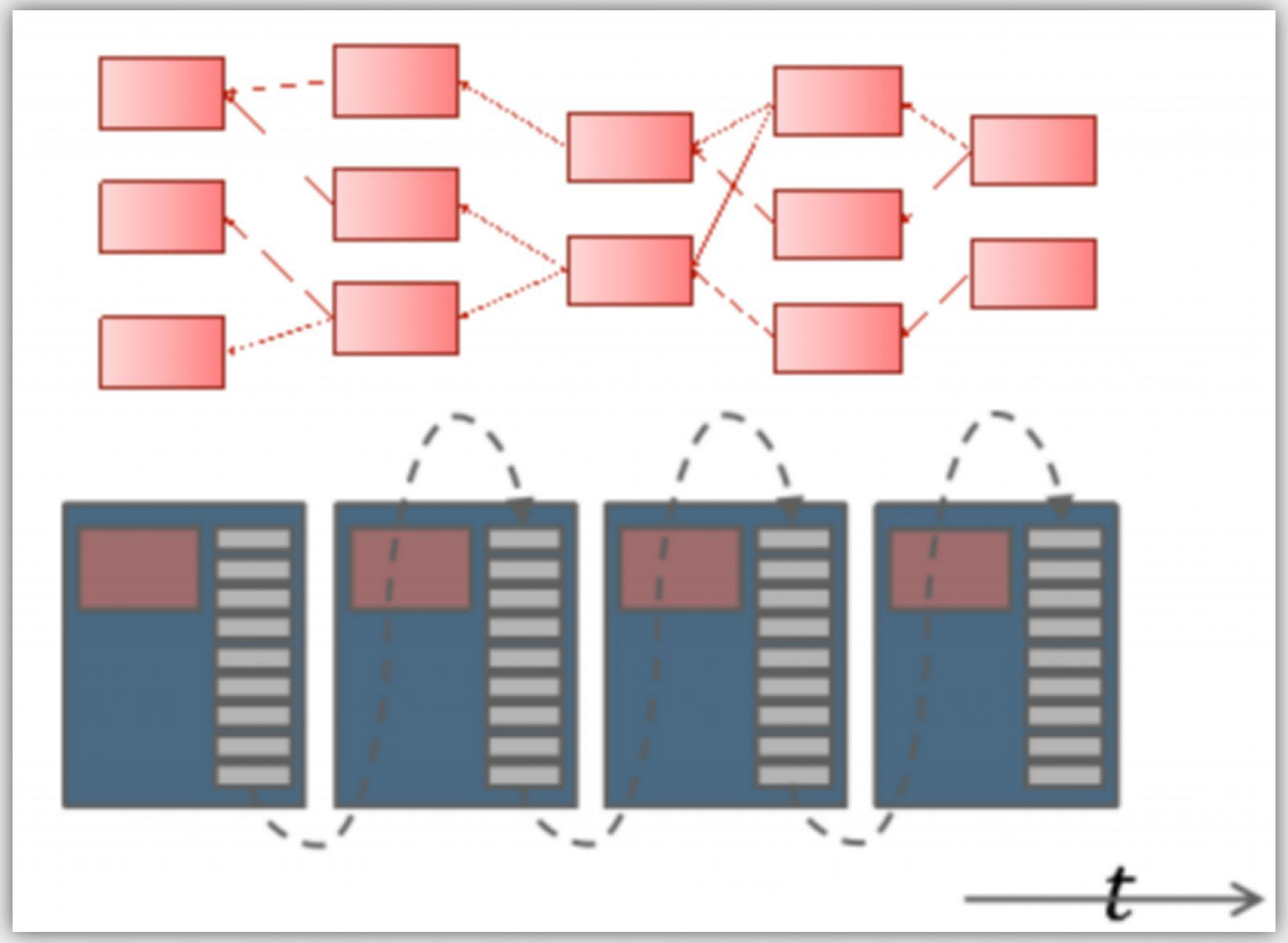
没有中心节点，如何阻止双花?



双花的避免

1. 两个矛盾的交易，如果能够排序的话，前面的交易确认，后面的交易不确认，作废
2. 确认的交易都构成一条链（区块链）
3. 这个链还可以被记上标记，第0块，第1块（创始区块？）

我们账本的形状



交易网络，部分交易未确认

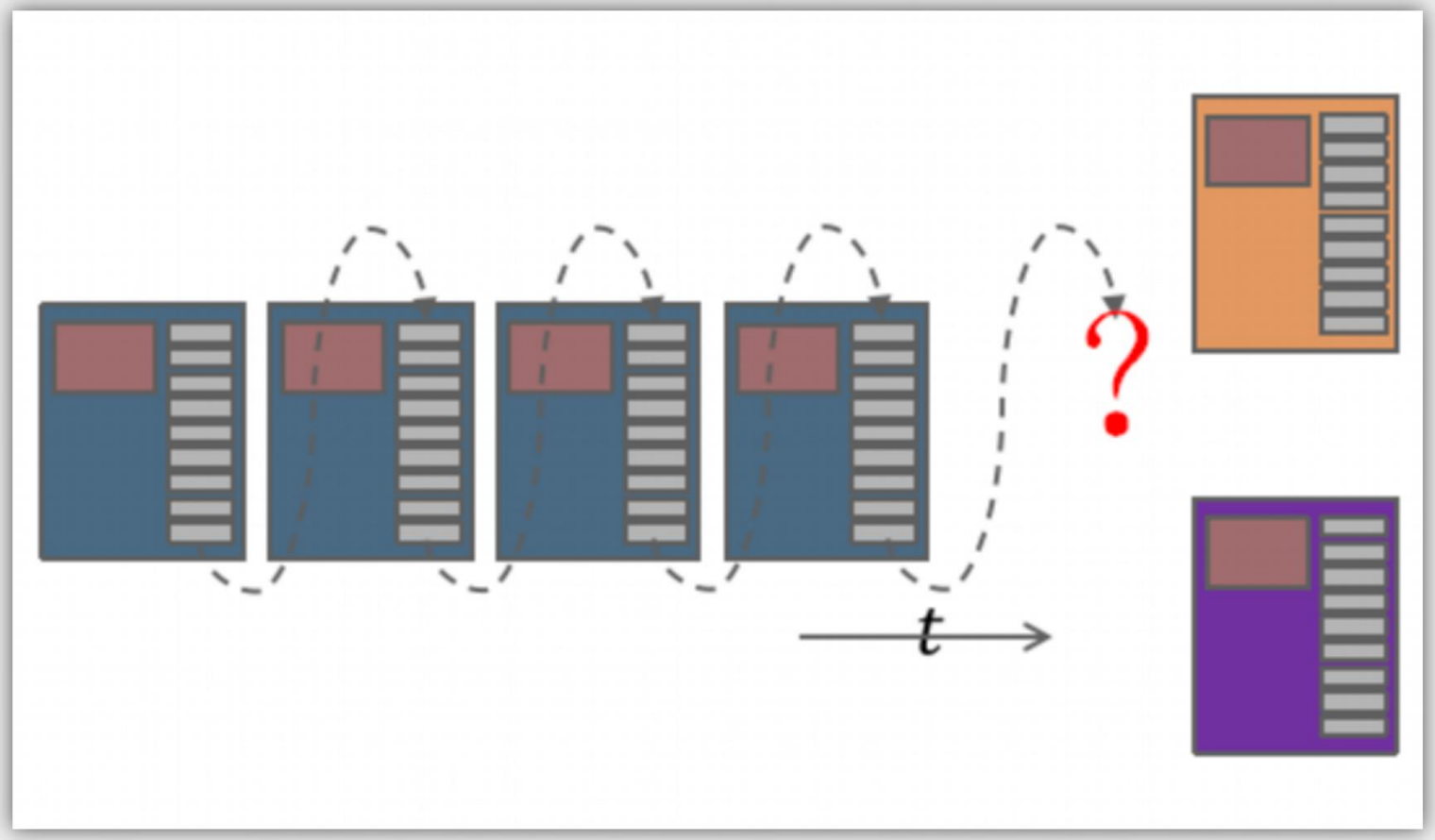
确认的交易放入区块链中

期望

1. 所有的确认的交易都一样的，即区块链上面的东西都是一样的
2. 但是，网络有延迟，每一个人拿到的块可能不一样，交易也不一样。
3. 上面的交易网络和下面的区块链都有可能是不一样的

为达到期望，怎么做?

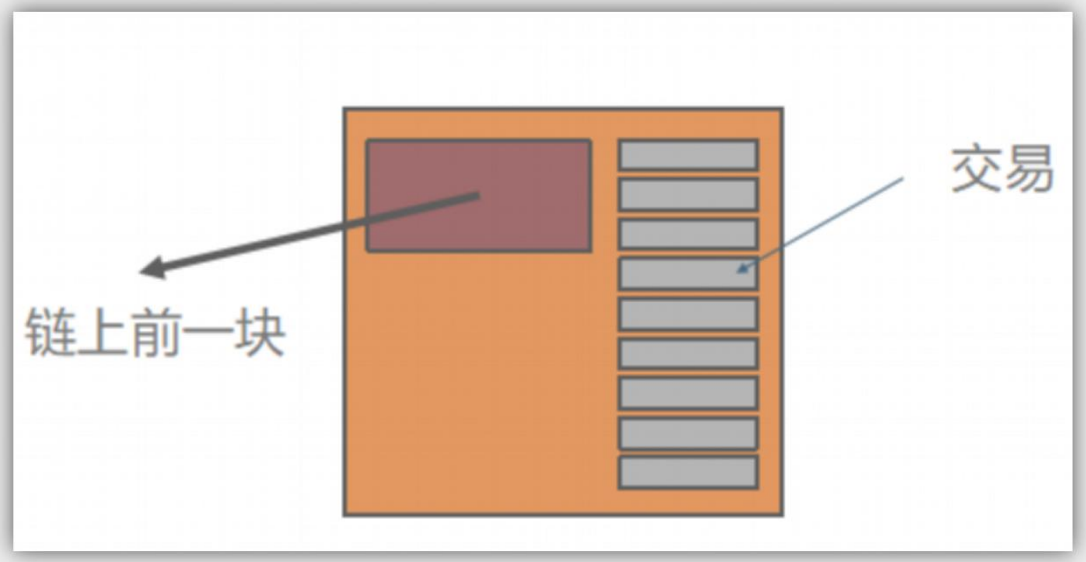
达成共识，以相同的顺序记录相同的交易



来来来，大家商量一下下一个块该放啥?绿色的?紫色的?

什么是块

1. 交易排序没问题，啥是块？
2. 由交易组成的块，为了性能，一批一批确认
3. 组块自己不能有矛盾
4. 组成块之后别人还可以验证



总结

1. 数字货币有双花问题
2. 防止双花要有全局的顺序账本
3. 区块链就是全局的顺序账本

布置作业

- 必做内容
- 了解区块链双花问题

EDU

CSDN学院　IT实战派