EDU

CSDN学院　IT实战派

比特币和区块链的相关技术细节

比特币的账户和交易

讲师：康烁

本节目标

1. 了解比特币的账户模型
2. 了解比特币的交易过程

比特币的UTXO以及对比传统账户模型

UTXO模型

1. UTXO – Unspent Transaction Output 未支出的交易输出
2. 上一笔交易将比特币汇至某一地址，这笔比特币可长期存储，直到该地址的主人要将款项汇至下一个收款人。在某笔款项尚未被提出汇至下一个地址之前，这笔款项被称为UTXO

传统的账户模型

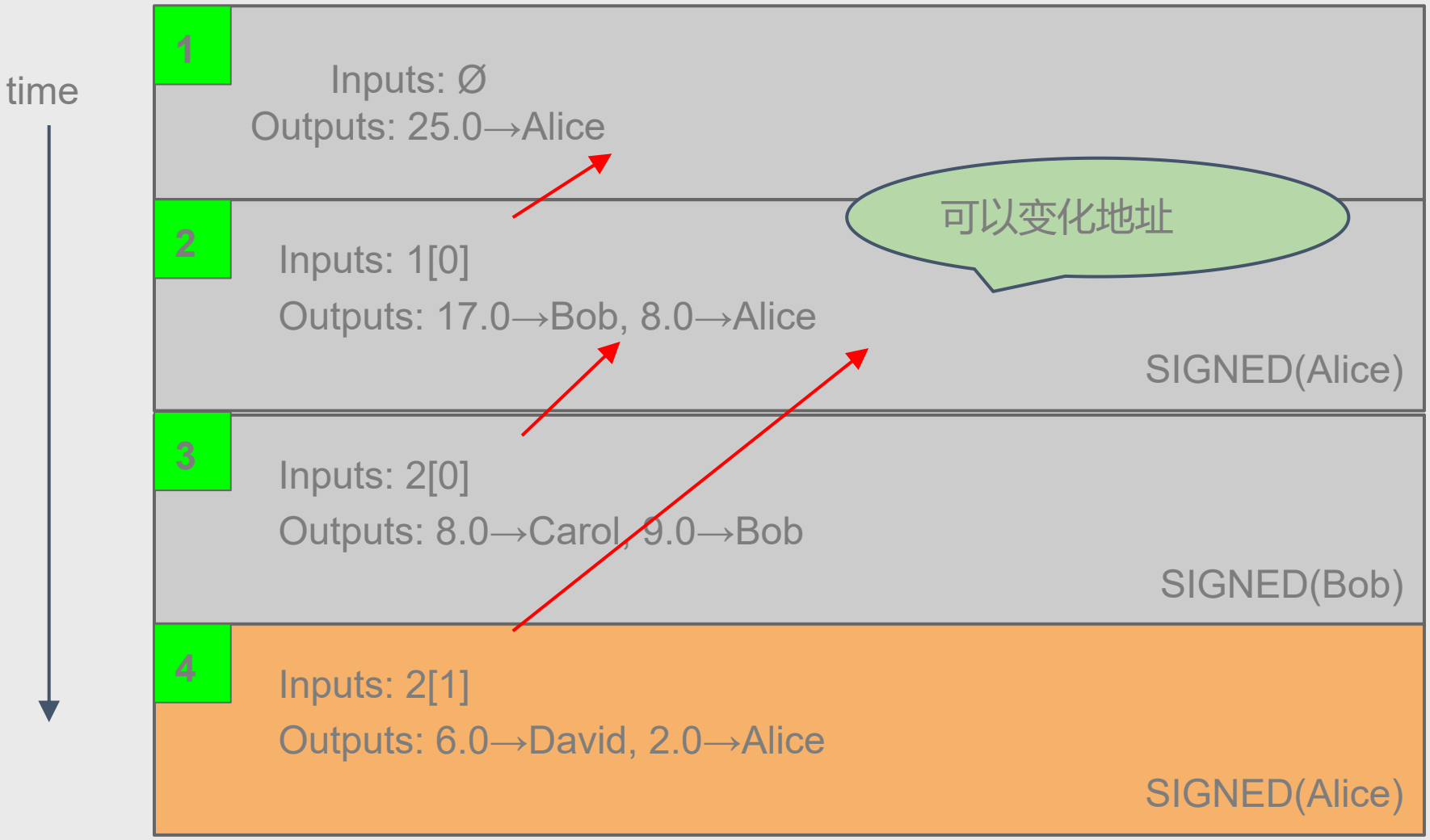
优点

原子性，或成功，或失败，无中间状态；可并发；消耗存储空间较小

缺点

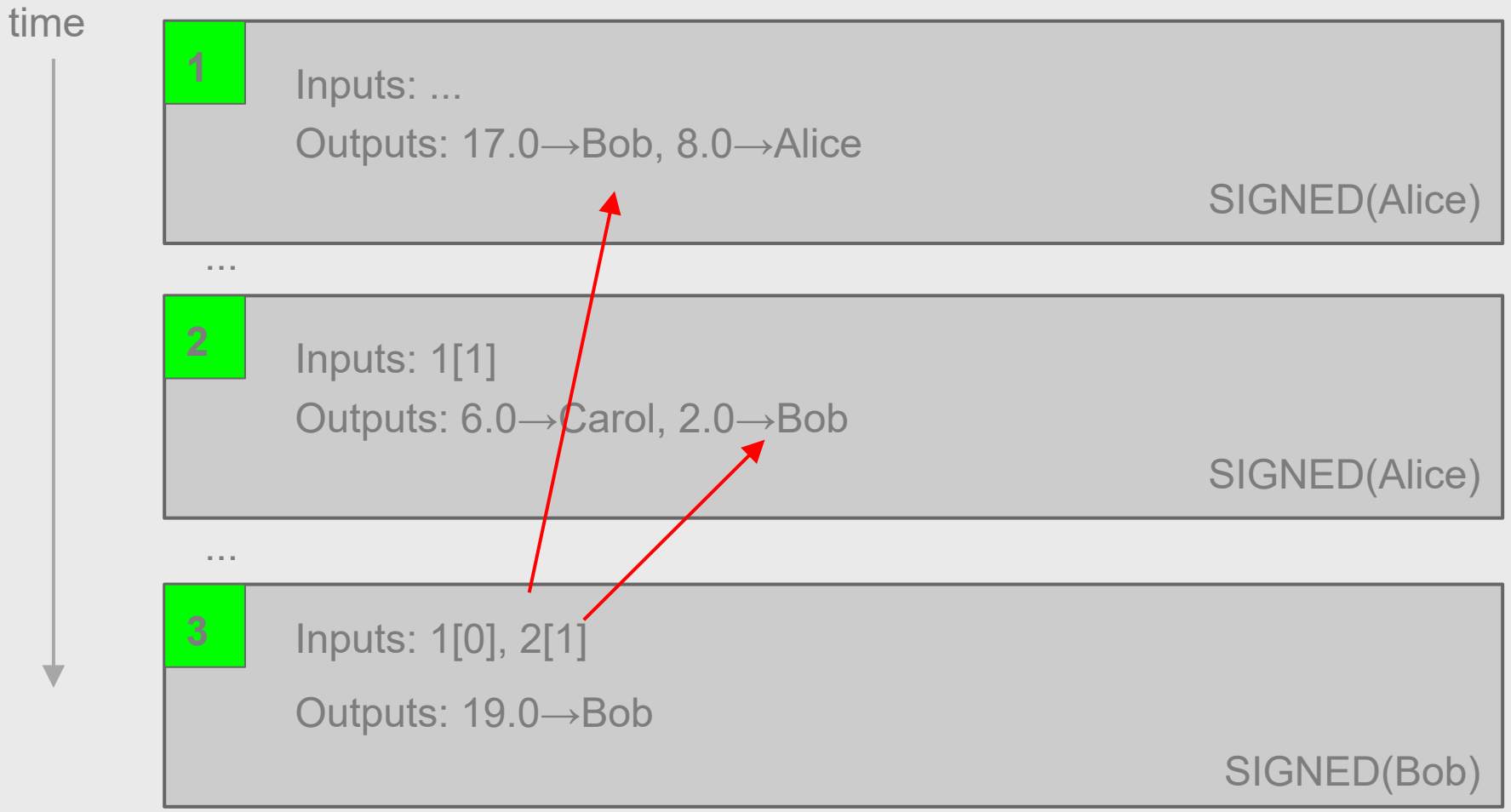
实现较为复杂；UTXO 无状态，若账户中需要存放复杂状态（如智能合约），则无法支持

简化交易过程：每个区块仅一个交易

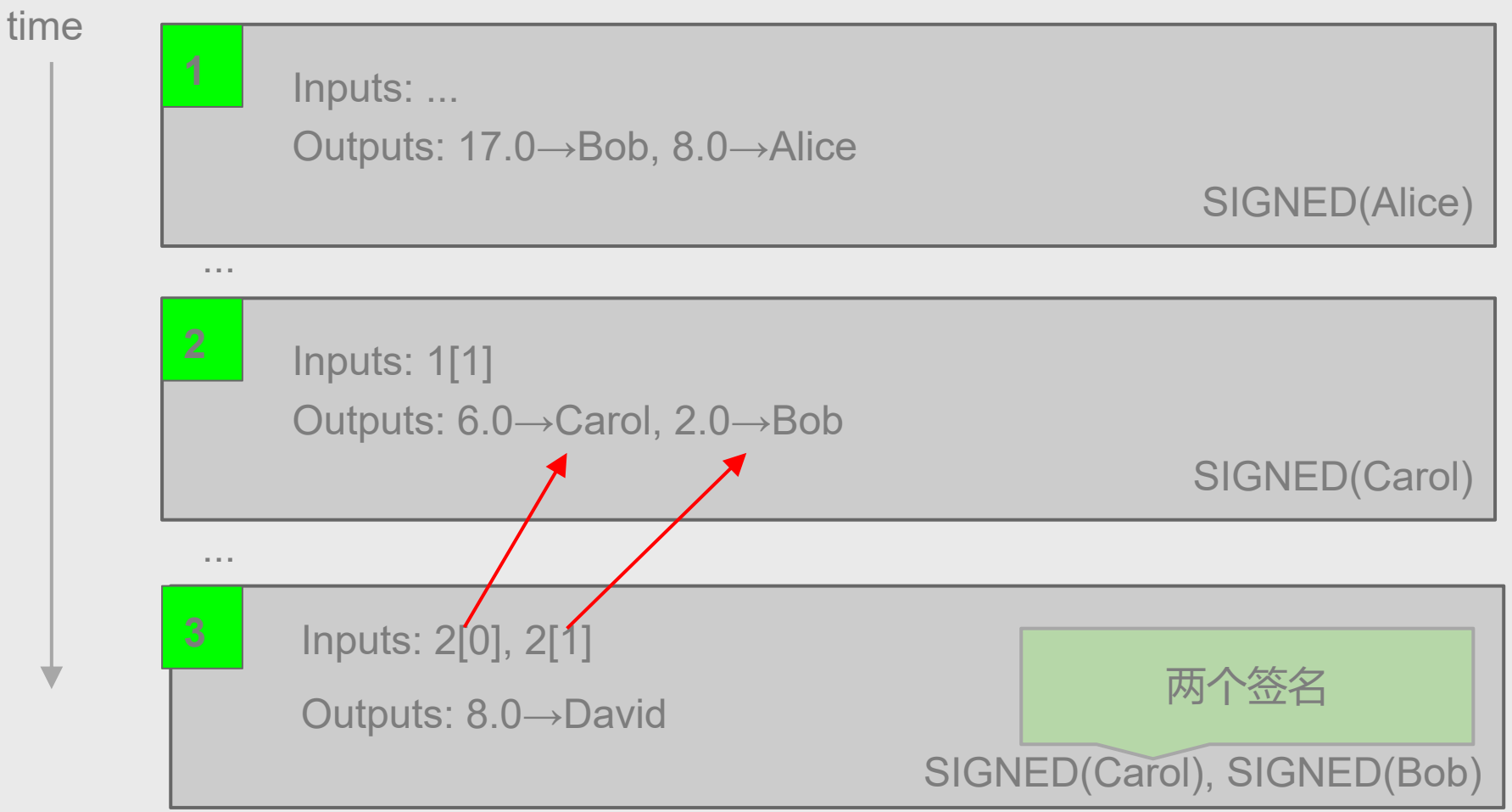


在实现中，后一个交易用哈希指针指向前一个交易

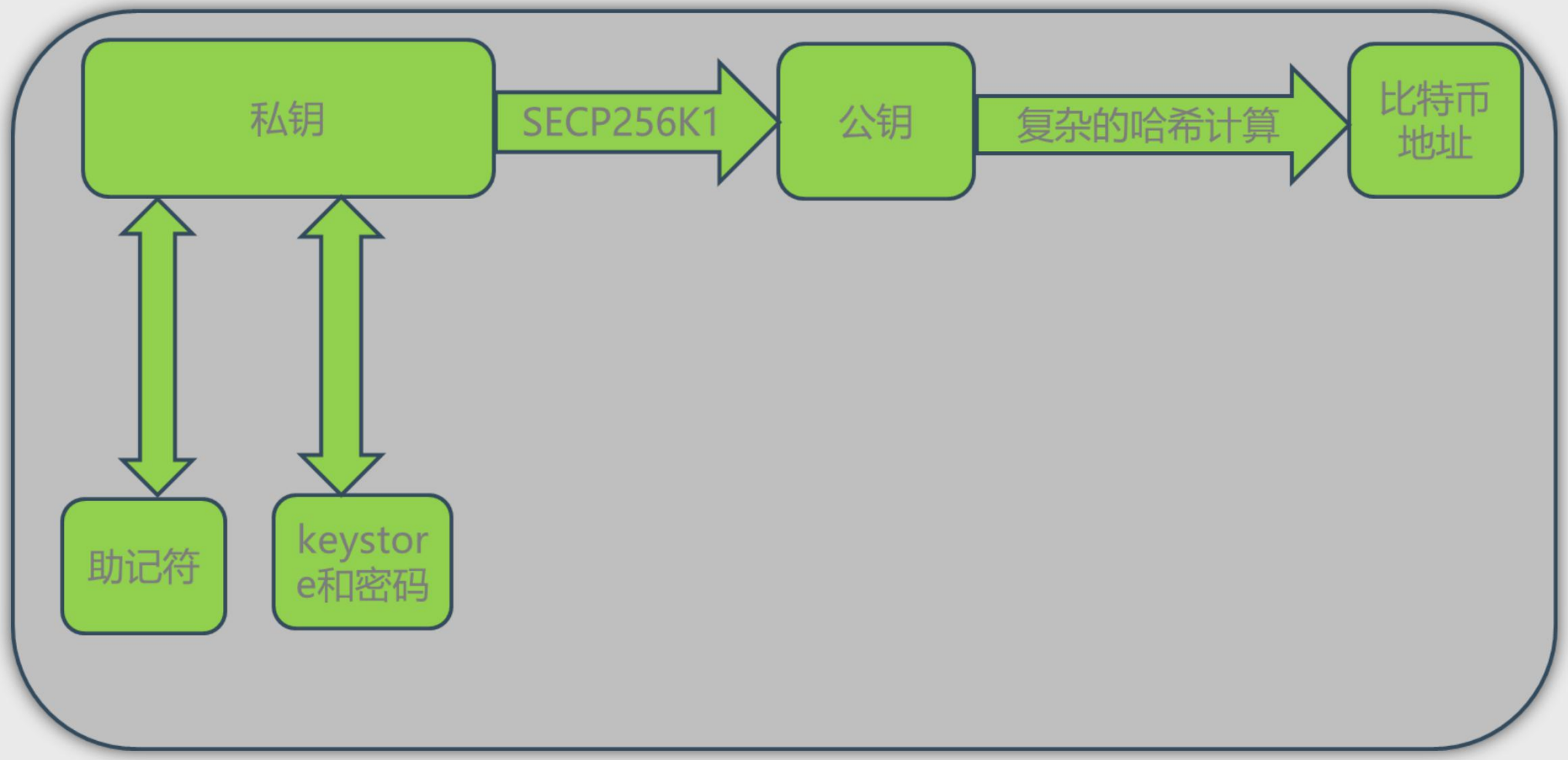
合并多笔交易的输出进行支付



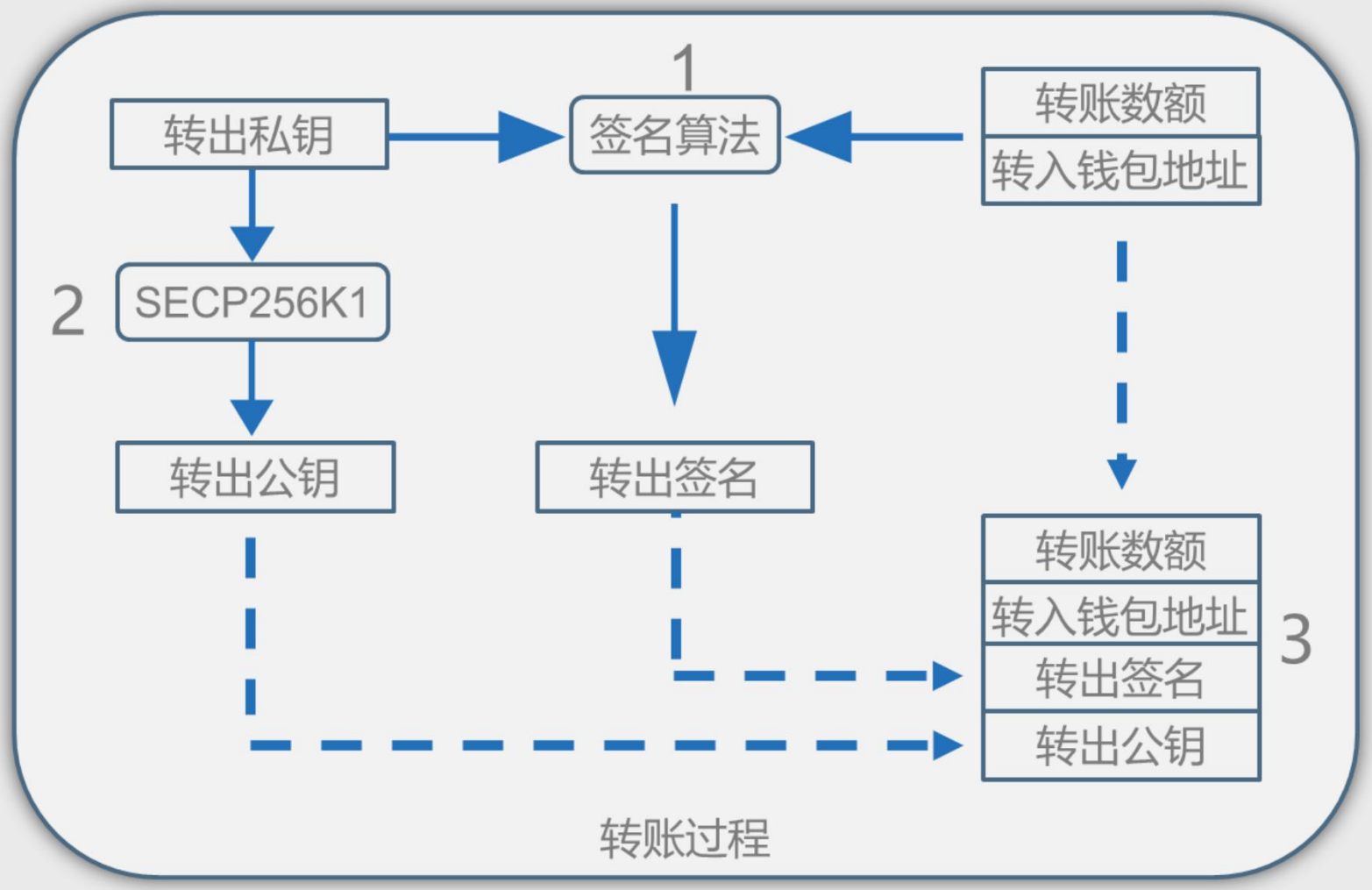
多人联合支付



比特币的地址

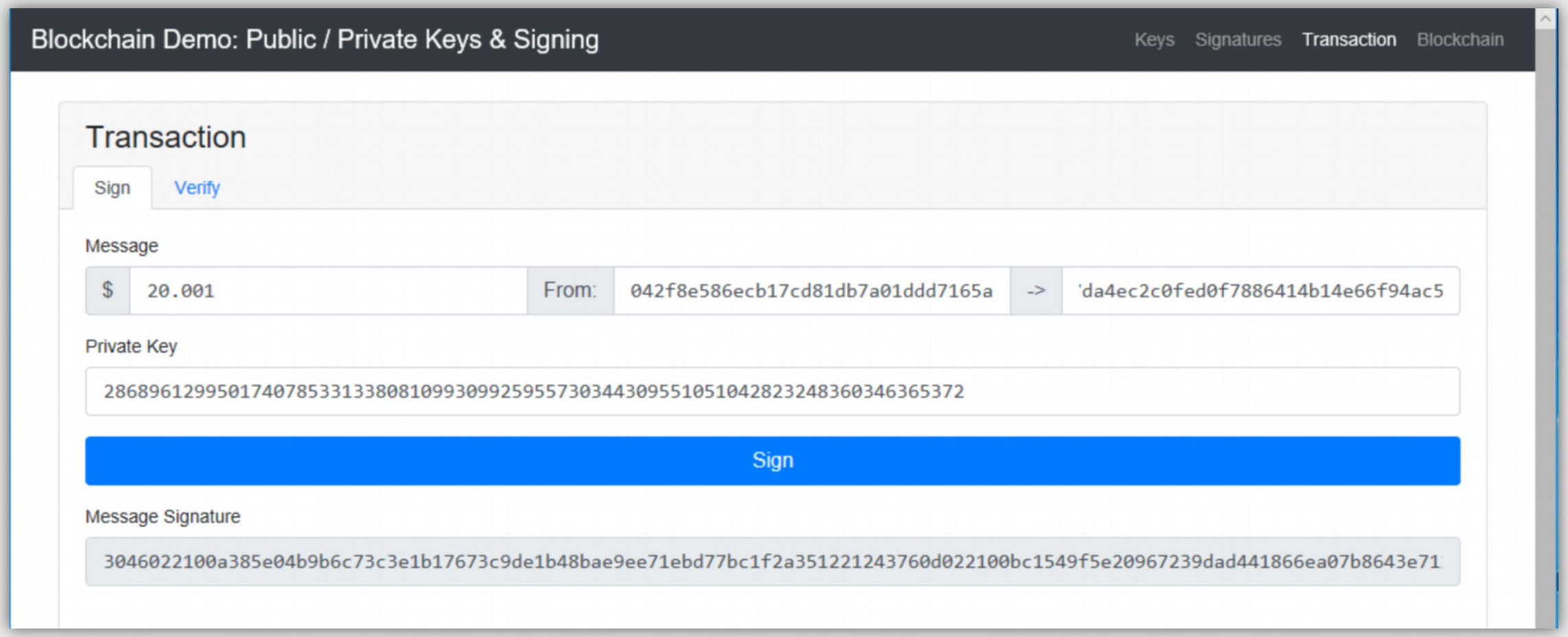


转账过程



Demo：给交易签名

演示地址：https://anders.com/blockchain/public-private-keys/transaction.html



总结

1. 比特币使用UTXO来记录账户余额
2. 比特币的交易脚本的类型和结构

布置作业

- 必做内容：
- 了解比特币的账户模型

EDU

CSDN学院　IT实战派