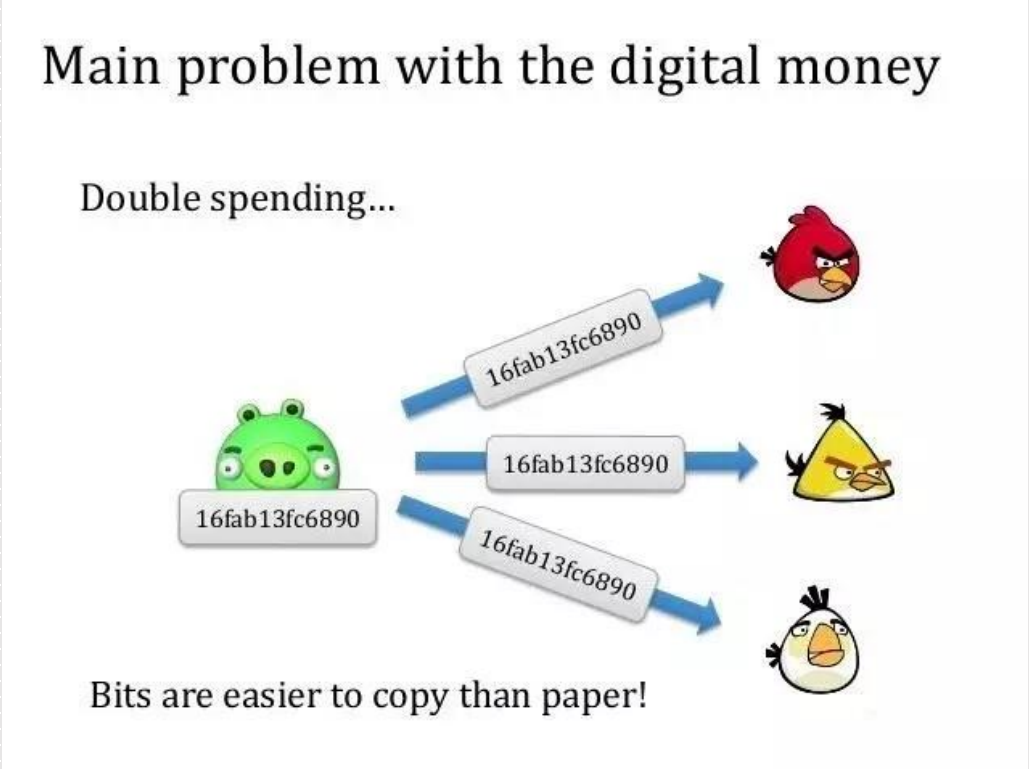
2.5 双花问题和UTXO的精妙

01 双花问题

一笔钱被花费了两次甚至更多次，也叫“双重支付”。

在**数字货币系统**中，数字资产本质上是以互联网为基础的虚拟数字，简单来说所谓的数字资产其实就是一串字符，因此它**很容易被复制**或者多次发送使用。在这种情况下，如果没有中心机构的存在，人们并不能确定一笔资产是否已经被花掉，这就导致系统可能存在同一笔数字资产因不当操作被重复使用的情况。



02 如何避免“双花”？

支付宝

微信支付

传统电子支付：

- 依赖于第三方信任机构
- 对数据进行中心化管理，并通过实时修改账户余额来防止“双花”的出现

弊端：人类需要为交易中第三方验证支付巨额费用。

03 如何避免”双花”?

比特币系统:

- 矿工在生成区块的时候，会从网络上收集交易信息，交易信息中包含了付款人的私钥签名。
- 矿工首先会验证签名是不是正确的，只要是正确的签名就被认为是付款人认可的支付。
- 然后矿工会从以前的区块链中追溯，看看付款人这次消费的比特币是不是以前没有被消费过。
- 然后记录下付款人可用的比特币余额。

这个过程也被称为**UTXO机制**。

04 比特币中的UTXO机制

- **UTXO**是Unspent Transaction Outputs的缩写，全称叫做“尚未使用的交易输出”。
- **U**代表Unspent，表示未支付的或尚未使用的，“尚未支付”指的是这个交易输出还没有出现在其它交易的输入端。
- **TX**是transaction的缩写，交易是从一个比特币钱包向另一个钱包转账，是唯一可以改变比特币所有权的方式，包含了输入、数目和输出这些基本内容。
- **O**是Output，是输出的意思，TXO连起来就是指交易输出。

05 比特币中的UTXO机制

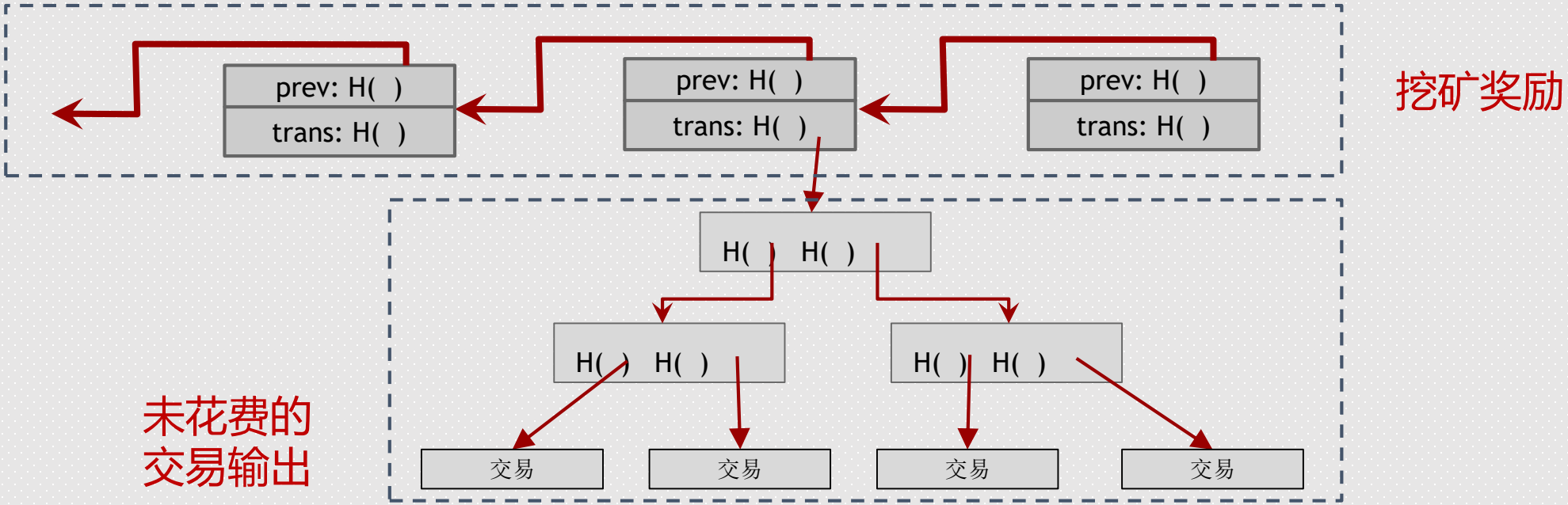
比特币里并没有用户帐户的概念。

我们说自己有多少比特币实际上是指的我们拥有所有权的那些UTXO中所指明的比特币的数量。

Alice有10个比特币，本质上来说其实是当前区块链账本中，有若干笔交易的UTXO项收款人写的是Alice的地址，而这些UTXO项的数额总和是10。

06 比特币交易

比特币的分布式区块链账本，就是由一笔一笔的交易形成的，每一笔交易都要花费一笔输入，产生一笔输出，而其所产生的输出，就是“未花费过的交易输出”，也就是UTXO。



07 比特币交易

比特币交易遵守几个规则：

第一，除了 coinbase交易之外，所有的资金来源都必须来自前面某一个或者几个交易的 UTXO。

第二，任何一笔交易的交易输入总量必须等于交易输出总量，等式两边必须配平。

08 UTXO举例

Coinbase交易 交易号：#1001			
交易输入	交易输出（UTXO）		
	第几项	数额	收款人地址
挖矿所得	（1）	12	Alice的地址

普通交易 交易号：#2001			
交易输入	交易输出（UTXO）		
资金来源	第几项	数额	收款人地址
#1001（1）	（1）	2	Bob的地址
	（2）	10	Alice的地址

普通交易 交易号：#3001			
交易输入	交易输出（UTXO）		
资金来源	第几项	数额	收款人地址
#2001（1）	（1）	2.5	Jimmy的地址
#2001（1）	（2）	**7.5**	Alice的地址