中本聪在比特币白皮书一开始就引入了“电子硬币”概念，并把它定义为“一连串的数字签名”，这就是比特币交易的基础，可能也是比特币之所以成为“币”的原因。

比特币采用了被称为UTXO的交易模型，你可能在前文中已经读到。作为一本非技术类读物，本书不打算仔细讲解这一交易模式，但可将它类比成日常使用的硬币、钞票等现金支付方式，以帮助理解。

假设买一杯奶茶需要支付32元，如果用微信钱包、支付宝或银联等电子支付的话，那么非常简单，直接扣除32元即可，完全不用担心零头的问题。但是，如果我们用现金支付，就有可能出现以下几种情形。

• 我们给店家32枚1元硬币，这时候正好不用找零，但大部分时候我们不会带这么多硬币在身上。

• 我们给店家3张10元钞票，外加2枚1元硬币，这样也不需要找零。

• 我们给店家4张10元钞票，店家找给我们8枚1元硬币。

• 我们给店家1张100元钞票，店家找给我们1张50元钞票、一张10元钞票，外加8枚1元硬币。

UTXO就是类似上述现金支付找零的方式，只不过它并不是“零头”本身，而是一个“找零”记录。

比特币的这一设计思路是：只记录交易，不记录最终状态。这种设计的一个最大的好处就是比较容易验证，我们仍然用现金消费来类比：当我们要买一杯32元的奶茶时，我们看下钱包，如果发现所有钞票、硬币加起来也不足32元，我们马上就知道自己的钱不够，而要知道购买完东西后还剩多少钱，我们只需把钱包里没花掉的钱相加即可。

因此，比特币的交易并不是大家想象的转账方式——把A账户的余额减少一点，对应把B账户的余额增加一点。比特币的系统里面并没有一个“账户余额”的东西存在，用户每次在比特币钱包里看到的余额其实是数字钱包根据区块链上的数据（UTXO）计算出来的（见图1）。从某种角度上来说，比特币的系统里并不存在真正意义上的“币”，而只存在UTXO，“币”仅仅是计量上的概念。

UTXO与账户余额的体系相比更复杂，可以表达的状态和附加信息更少，扩展性不足。但它对于比特币这样一个以点对点的电子现金为设计目标的系统来说已经足够

，而其高效率、灵活、更容易防止双重花费攻击等优点更为重要。大量基于比特币代码分叉的区块链都采用了类似做法，而更关注应用和扩展能力的区块链，例如以太坊、Hyperledger
Fabric、ArcBlock等，都无一例外还是采用了账户模型的设计方式。