UTXO是比特币交易的基本单位  
  
UTXO（Unspent Transaction Outputs）是未花费的交易输出，它是比特币交易生成及验证的一个核心概念。交易构成了一组链式结构，所有合法的比特币交易都可以追溯到前向一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。所有的未花费的输出即整个比特币网络的UTXO。  
  
比特币规定每一笔新的交易的输入必须是某笔交易未花费的输出，每一笔输入同时也需要上一笔输出所对应的私钥进行签名，并且每个比特币的节点都会存储当前整个区块链上的UTXO，整个网络上的节点通过UTXO及签名算法来验证新交易的合法性。这样，节点不需要追溯历史就可以验证新交易的合法性

TX     : Transaction（交易）  
TXO  : TX output（交易输出）：包含一个value值和一段脚本，该脚本规定了谁有权使用这笔交易（比如需要私钥签名）。  
  
UTXO： Unspent TXO（未花费的交易输出）：只有对“尚未使用过”的交易签名才能是有效签名。  
  
数字货币无法像金属货币（比如黄金）那样，仅靠物理转移即可转移所有权————即当A将一份黄金交给B后，A必然不再拥有这份黄金。  
而A将一份数字货币转给（签名）B后，A仍可以把同一笔交易转给C，因为A掌握私钥，这两份签名均为有效签名，这就构成了“双花”。因此必须有一种机制来确保每笔交易只能使用一次，即只有对“尚未使用过”的交易签名才能是有效签名。  
  
以往的密码学货币无法有效解决双花问题，因而无法摆脱对第三方中心化机构认证的依赖（第三方信任）。  
2008年底，一个自称中本聪的人提出了一个构想，用PoW区块链的方式来摆脱第三方信任。  
2009年1月份，一个名为“比特币”的系统开始运行，第一个可以不需要“信任”的电子现金系统出现了......

通俗易懂地来讲，UTXO就相当于是你的加密支付宝红包口令，是比特币的容器。  
而私钥是解密这个口令红包的关键。有私钥者有UTXO中的币的控制权。  
一个币地址可以有一个或多个UTXO，看分几次收币。  
  
想要像别人发比特币，就要用你的私钥签名来“解冻”一个或多个UTXO。  
发给别人，也是成为别人地址的UTXO。

下面我们说以太坊的UTXO。以太坊的确是在考虑引进UTXO，但是此UTXO非彼UTXO。并不是像大家想象的那样，用UTXO来替换现有的账户模型。首先以太坊为智能合约而设计，其账户模型里除了有余额（balance），还有智能合约代码，还有nonce（为防止重放攻击），以及自定义的存储。把这些换成UTXO显然不合适，因为UTXO胜任不了。比特币的UTXO里只有一个简单的属性：余额（balance）。

那么以太坊的UTXO是指什么呢？这就是以太坊的另一个话题了：分片（Sharding）。分片是扩展以太坊、增加TPS的有效方法，目前正在社区里被广泛讨论和研究。目前的以太坊的工作模式是所有节点（比如共16万个）同时验证所有交易，实际上这是极度低效和没有必要的一种模式。为了保证一致性，如果我们按照地址的前4位来分片，可以把所有地址分成16片。这样每个交易只需要其中1万台节点验证便可通过。如果一个交易涉及的账户都在同一片区并没有什么问题，但如果涉及到不同片区问题就来了。

为了解决不同片区之间的交易问题，以太坊设计出了称为收据（receipt）的工作模式。而这个收据的模式和UTXO类似，故而也称为以太坊的UTXO。

既然此UTXO并不是指替换当前账户模型，变成比特币模式的UTXO，那么是不是说明当前账户模型就没有问题呢？也不是！当前账户模型的确存在一些弊端。

以太坊中以太币的转移安全性不如比特币高。下面是一个真实的例子。一个网友请我帮忙，让我帮助从Yobit.net追讨258个ETH。原因是他从Yobit.net转移币到云币网账户时，发生了out of gas错误。云币网给出的目标地址是一个合约地址，而Yobit.net以为是个外部地址，交易设置的gasLimit为21000（这对于合约账户就不够了），因此发生了out of gas的异常。币的转移被取消，但是这个交易（Transaction）却是完成的。