



CyberKuber 白话区块链系列课程 1：流动的黄金 UTXO



前言

流动的黄金，这个比喻与谷歌的 TensorFlow 有点异曲同工，在 Ulord 系统里，就好像有很多的 UTXO 在流动。要想了解 Ulord 区块链的运行的基本原理，UTXO 是一个很好的切入点。





在 Ulord 的转账过程中，有一个特别值得一提的概念，叫 UTXO。了解过比特币的小伙伴应该比较清楚，UTXO 是比特币的原创，那么对于跻身于比特币系的 Ulord 公链来说，自然免不了涉及到这个天才设计。前段时间，在进行在 Ulord 主节点申请过程中，有一个环节就是要锁定 10000UT (UT 是 Ulord 公链的通证，UlordToken 的缩写)，作为主节点的基本要求，然而，这看似十分简单的动作，却闹出了不少“笑话”，一些小伙伴为了凑齐 10000UT，转入转出，来来回回折腾了无数次，最后还是求助技术人员才把这“庞大的工程”完成。那么，到底为什么会出现这种本不应该出现的难题呢？仔细想来，罪魁祸首应该就是这个 UTXO！

账户余额模型

在详细介绍 UTXO 之前，我们先从熟悉的东西入手，看看传统的账户余额模型是怎么工作的。在现实生活中，银行卡采用的账户余额模型，想想下面一种场景：Cyber 要给乐淘淘转 100 元。





首先，Cyber 有一个账户，假设里面有余额 500 元，乐淘淘也有一个账户，假设有余额 200 元。当 Cyber 付给乐淘淘 100 元时，系统会做如下操作：

1. 检查 Cyber 账户余额为 500 元，大于 100 元，将 Cyber 账户里减去 100 元（如果加上手续费，Cyber 的账户的实际余额应该小于 400 元）；
2. 在乐淘淘的账户里增加 100 元（乐淘淘的账户余额为 300 元）。

账户余额模型可以通过中心化（传统银行系统）或者去中心化（以太坊）的方式实现，不同点主要是在于谁来记账。

UTXO 模型

现在来看看 UTXO，UTXO 是 Unspent Transaction Output 的缩写，其中 TX 表示 Transaction。相似的应用场景，Cyber 要给乐淘淘转 100UT。在 UTXO 模型中，系统会有哪些流程呢？



首先，Cyber 有一个 UT 钱包，钱包里面可使用的 UT 是 500。乐淘淘有一个 UT 钱包，钱包内有 300UT。注意了，需要敲一下桌子！Cyber 的 UT 钱包里面的 500UT，



其实在 Ulord 区块链上记录的是一笔笔的转账,假设 Cyber 的 UT 来源是李雷转入的 200UT 和韩梅梅转入的 300UT。这个时候, Cyber 拥有两个 UTXO 的使用权,一个是 200UT,一个是 300UT。每一个 UTXO 是一个整体,只能作为一个整体使用。好的,接下来,我们再来看看, Cyber 给乐淘淘转 100UT 时, Ulord 系统做了什么:

- 1.选择一个大于 100UT 的 UTXO,这里选择 200UT 的这个 UTXO;
- 2.创造一个 100 的 UTXO 给乐淘淘,同时创造一个 99.99UT 的 UTXO 给 Cyber 作为找零(这里假设系统收取 Cyber 的转账手续费为 0.01UT,实际上没这么高,多少还可以自己调节!)。

我们再来看看转账结束后两个人的 UTXO 变化, Cyber 拥有两个 UTXO:一个 99.99UT,一个 100UT;乐淘淘增加了一个 100UT 的 UTXO。



从上面的例子我们可以看到,其实 UTXO 就像纸币,每一个 UTXO 都有自己的面值,但和纸币不同的是,在一次支付过程中有旧的 UTXO 被销毁,新的 UTXO 被生成。



UTXO 的面值是变化的，转账多少，新生成的 UTXO 面值就是多少。对比而言，纸币在支付的过程中，没有新的纸币产生，而是把支付方的纸币给到收款方，找零是由收款方给到支付方，且纸币的面值是固定有限的。

说到这里，大家应该大概知道了 UTXO 模型的一些特性，这里我总结一下：

1. 每一个 UTXO 只能以一个整体使用，像使用一张纸币；
2. 一个交易过程，有旧的 UTXO 销毁，新的 UTXO 产生，销毁与产生的 UTXO 等值（不考虑手续费）；
3. UTXO 有自己的“面值”，每次支付可以用掉多个 UTXO，保证支付足够多的 UT。

结束语

随着我们对 UTXO 的了解，又产生了一个新的疑惑，既然每个交易都是有 UTXO 的销毁与产生，且输入与输出的 UTXO 面值相等（不考虑手续费的情况下），以保持系统内部 Token 的数量恒定，那么这些 Token 是怎么来的呢？这好像类似于一个鸡生蛋的问题。其中的缘由就是 coinbase 交易，关于 coinbase 的相关介绍，请关注下一篇文章《CyberKuber 白话区块链系列课程 2：动力的源泉 coinbase 交易》。