目录

简述

在比特币系统上其实并不存在“账户”，而只有“地址”。只要你愿意，你就可以在比特币区块链上开设无限多个钱包地址，你拥有的比特币数量是你所有的钱包地址中比特币的总和。比特币系统并不会帮你把这些地址汇总起来形成你的账户。由此就具有很高的隐私性，他人无法通过一个地址找到你的其他地址，避免了钱财过度集中在一个账户上。

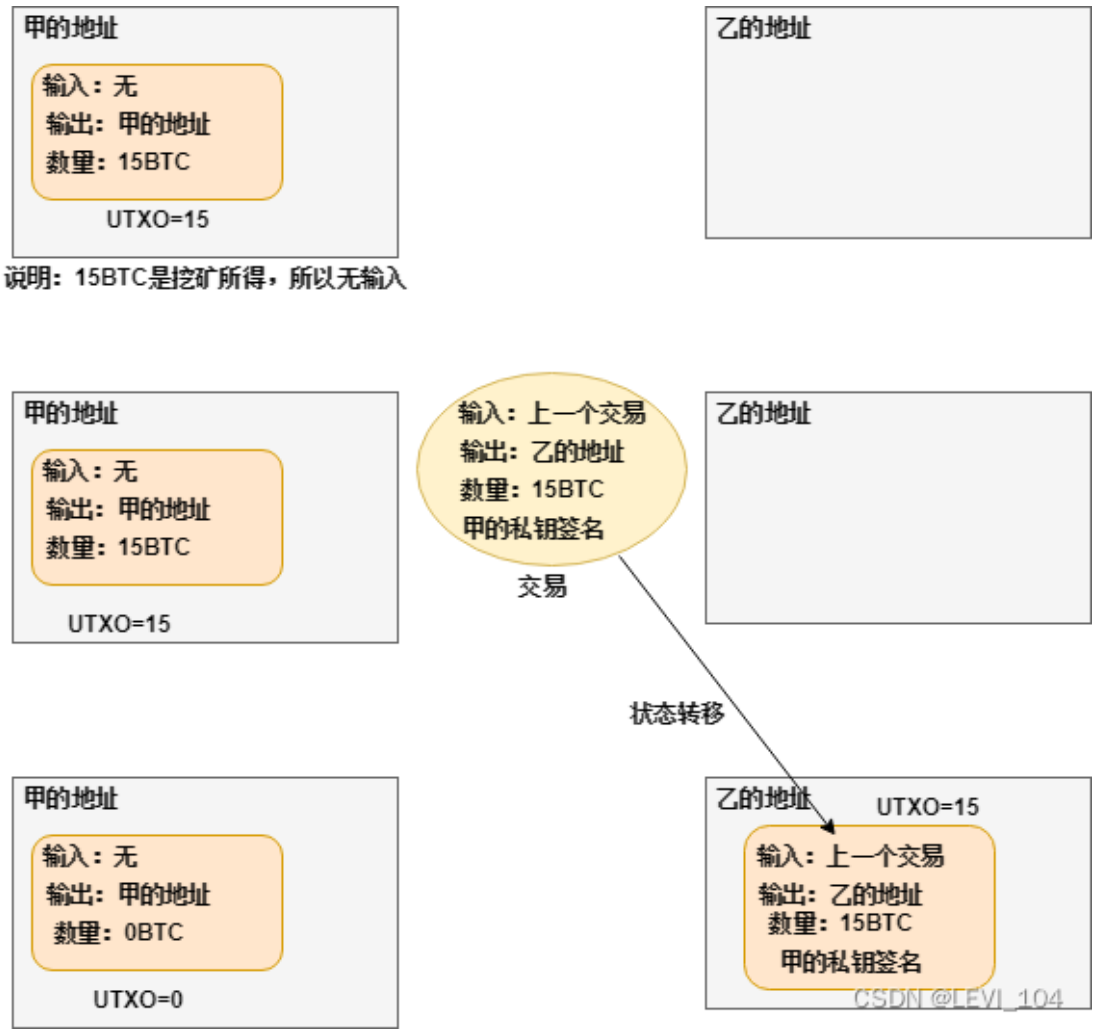
情景引入

假设我有 15 个比特币【这其实意味着，之前有一个交易把这些比特币转入我的地址），这个交易的输出（即 8 个比特币）未被使用，我拥有了这 15 个比特币】。

现在，我要发起一个转账交易，这个交易中的输入是让我拥有这些比特币的上

一个交易。
我要转账给你，我做的是，对让我拥有这些 15 个比特币的上一个交易进行签名，把这一新转账交易的输出地址设置为你的钱包地址。

这样，我就发起了一个转账支付交易。等矿工将这一交易打包进新的区块，转账交易完成，这 15 个比特币就属于你了。你拥有的是你我这个交易的未使用的交易输出。如下图表示。



编辑

图 1-1

说明：（1）上图是假设甲没有上一笔交易的全新地址，15 比特币的来源是他挖矿所得。

（2）这里简化了交易过程，只讨论了将上一个交易的输出全部转帐的情况。如果试图转出上一个交易的输出的一部分比特币，则要进行略复杂的处理，如下：

按照比特币系统的设计，比特币交易还要遵循一个原则：每一次交易的输入值都必须全部花掉，不能只花掉部分。

比如，我要转出比特币给你的钱包地址中只有 15 个比特币，那么很简单，我发起一个交易，把这 15 个比特币转到你的钱包地址中，我签名确认这个交易。但假如我的钱包地址中有 25 个比特币，那我发起的交易就不是转给你 15 个比特币，然后自己的钱包地址中还剩下 10 个比特币。这时，我发起的交易是：从我的钱包地址中转 25 个比特币给你，同时转 10 个比特币给我的地址。

UTXO 介绍

UTXO（Unspent Transaction Outputs）是未花费的交易输出，他是比特币交易的**最基本单元**，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根据签名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。现实世界中没有比特币，只有 UTXO

中本聪设计 UTXO 机制的原因

区块链是怎么记录比特币交易的？——记账。

怎么记账？——每个区块是由区块头和区块体组成，区块体中有账本，在账本上记就行了。

常规账户记账的问题

那如果交易特别多的话，记录的信息会不会很占内存？——如果像支付宝的账单、微信支付的账单那样，是很占内存的。比如，你有 10 元钱，花了 5 块钱，出来一个“-5 元”的账单；然后收到 3 元钱，又出来一个“+3 元”的账单；... ... 以此类推。那么计算余额时是这样计算的：“10-5+3=8（元）”。不但计算过程比较复杂，还很占内存。

有多占内存？——假设 BTC 和传统货币一样，使用账户余额系统，首先需要一个数据库，记录所有人的余额。这里假设全世界使用比特币的用户有 10 亿人，每个人每天交易 10 次，那么平均每秒余额变动将达 11 万次，如果按照这个频次继续下去，用不了多久相关数据就会撑爆线上的服务器。

解决方法

使用 UTXO。刚才讲的，支付宝、微信那种记账方式，是基于账户的记账方式。仍然举这个例子，通过使用 UTXO 记账方式。比如，你有 10 元钱，花了 5 块钱，出来一个“之前剩余 10 元，现在剩余 5 元”的 UTXO 账单；然后收到 3 元钱，又出来一个“上次剩余 5 元，现在剩余 8 元”；... ... 以此类推。那么这种模式下，即使你之前的账单丢失了，也能知道当前的余额。

可以这么说，UTXO 只记录了当前的**状态**，而不去记录交易的过程

交易的详细过程

coinbase 交易

Coinbase 交易是一种特殊类型的交易，通过创建新的 BTC 来奖励找到区块的矿工。由于创造了新的比特币，coinbase 交易没有输入，但是会产生一个或多个输出。就像所有正常输出一样，coinbase 交易的输出是新的 UTXO。

每个 UTXO 的历史都可以追溯到 coinbase 交易的一个或多个输出。

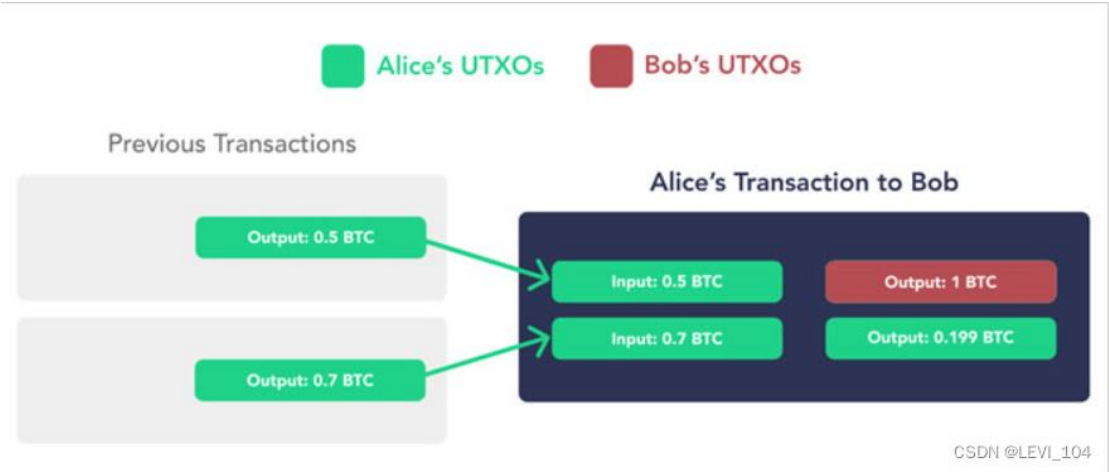
交易原理图

图 1-2：图片来源于知乎作者：悦诗 LY

UTXO 的拆分和组合

一个比特币交易可以包含任意数量的输入和输出。因此，用户可以任意组合和拆分 UTXO 来完成任意金额的付款。

例如，Alice 持有两个 UTXO，分别价值 0.5 BTC 和 0.7 BTC。当她向 Bob 支付 1 BTC 时，可以使用这两个 UTXO 作为输入，然后将 1 BTC 的输入发送给 Bob。



编辑

图 1-3：图片来源：网络引用

说明：（1）由于需要支付交易费，她无法给自己发送 0.2 BTC。（2）Alice 原来拥有的 1.2BTC 是未使用的，当她进行合法交易的时候，1.2BTC 全部转给 Bob，这 1.2BTC 就是使用过的。然后 Bob 会找零发送回 0.199BTC 给 Alice，而这 0.199BTC 对于 Alice 来说就是未使用过的。也是解决双花问题的关键。

⚠ 交易费不以交易输出（UTXO）的形式体现。它是通过输入值和输出值之间的差额推算得出。

UTXO 的优点

- UTXO 不能分割，只能被消耗，独立的数据结构大大减少了计算量。
- UTXO 配合地址使用，具备天然的匿名性，保证了账户的安全。
- 因为地址的存在，UTXO 的销毁和产生，都可追溯，很难伪造。
- 长期来看，UTXO 的数据占用更小，而余额系统会越来越臃肿。
- UTXO 设计与区块链账本是完全融为一体的 ：

区块链账本存储的是状态。以太坊是对比特币区块链的改进，在白皮书中，以太坊创始人维塔利克分析了比特币，他认为，“比特币账本可以被认为是一个状态转换系统（state transition system）”。以太坊也是采用这种状态转换系统的设计，但对之进行了改进。

- UTXO 设计易于确认比特币的所有权：

如果采用传统的账户设计，当我要转账 8 个 BTC 出去时，为了完全避免造假，我们就需要逐一向上追溯，确认之前的每一笔交易，从而证明我的确拥有 8 个 BTC。采用现在的 UTXO 设计，要确认我拥有 8 个 BTC，只要确认上一个交易我的确获得了它们即可。通常只要上一个交易是真实的，我就的确拥有这些比特币。而我们都知道，一个区块经过 6 次确认，其中的交易可被认为是真实无误的。

所以大家看明白了吧，比特币不是具体的钱币，只是 UTXO 账单上的一个数。

UTXO 解决双花问题

- 如果采用账户和账户余额设计，Alice 要转账给 Bob，为了确保 Alice 的确有钱，我们需要核查她之前所有的交易。随着时间的推移，BTC 的交易越来越多，这个验证的难度会持续上升。
- 采用 UTXO 设计，我们只要沿着每个交易的输入逐级向上核查，直到查到这笔 BTC 的创币交易即可。随着时间的推移，这个核查也会变难，但变难的速度要远低于采用账户和账户余额设计。

见图 1-3

Alice 原来拥有的 1.2BTC 是未使用的，当她进行合法交易的时候，1.2BTC 全部转给 Bob，这 1.2BTC 就是使用过的。然后 Bob 会找零发送回 0.199BTC 给 Alice，而这 0.199BTC 对于 Alice 来说就是未使用过的。也是解决双花问题的关键。

同时，这种设计使得比特币系统作为一种电子现金系统有着非常大的可扩展性。当然，我们很快会看到，通常被认为是区块链 2.0 的以太坊没有继续采用 UTXO 设计，而是考虑到其他因素，采用了账户余额的设计，其代价正是中本聪可能已经考虑到的复杂性。

杂谈

最后，附上一段话。正如，中本聪在比特币白皮书上说：

It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is

not a problem here. There is never the need to extract a complete standalone copy of a transaction’s history.

“当一笔交易基于之前的多笔交易时，这些交易又各自基于多笔交易，但这并不存在任何问题。因为这个系统永远不需要提取一份所有历史交易的完整记录”