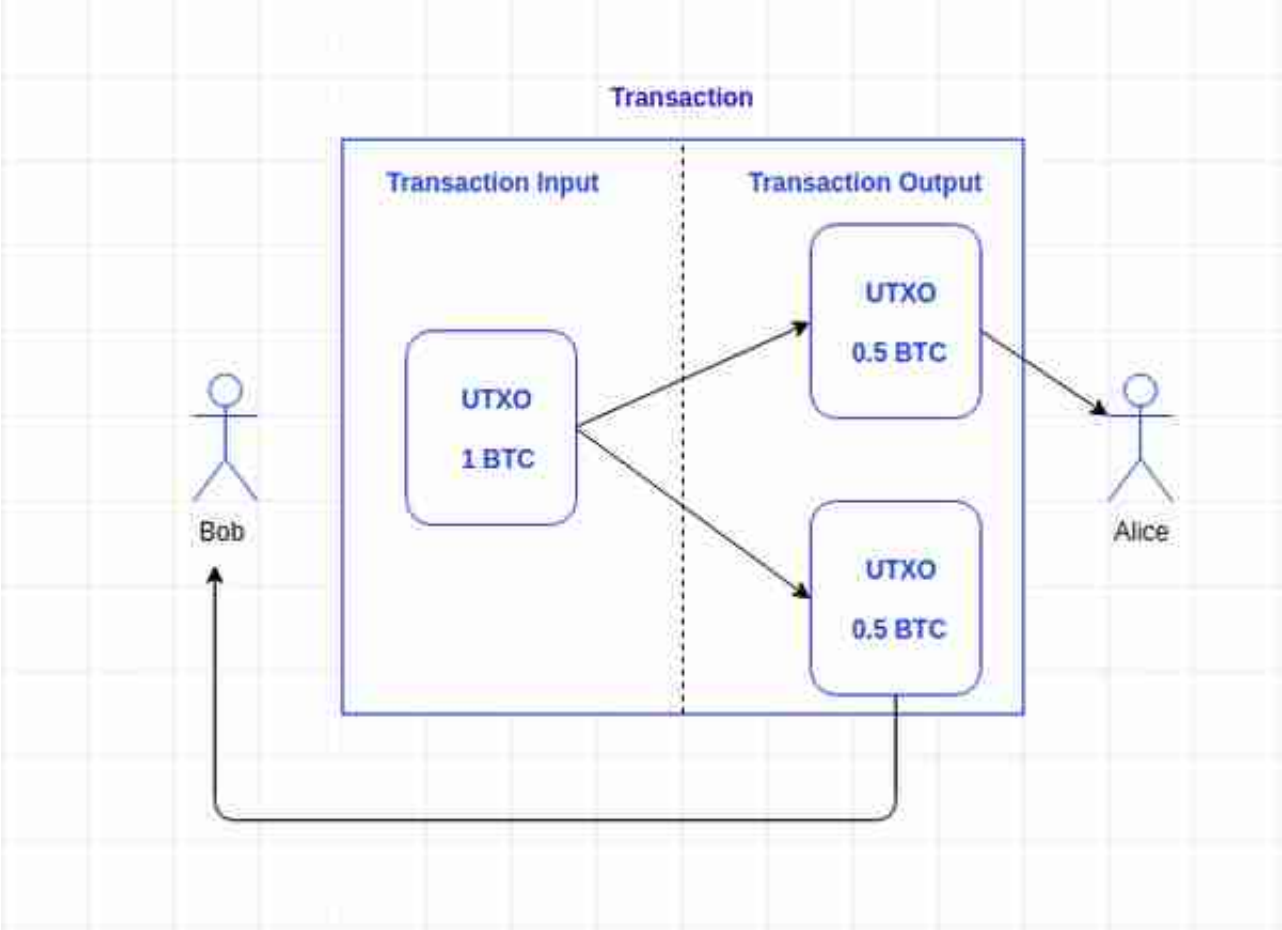
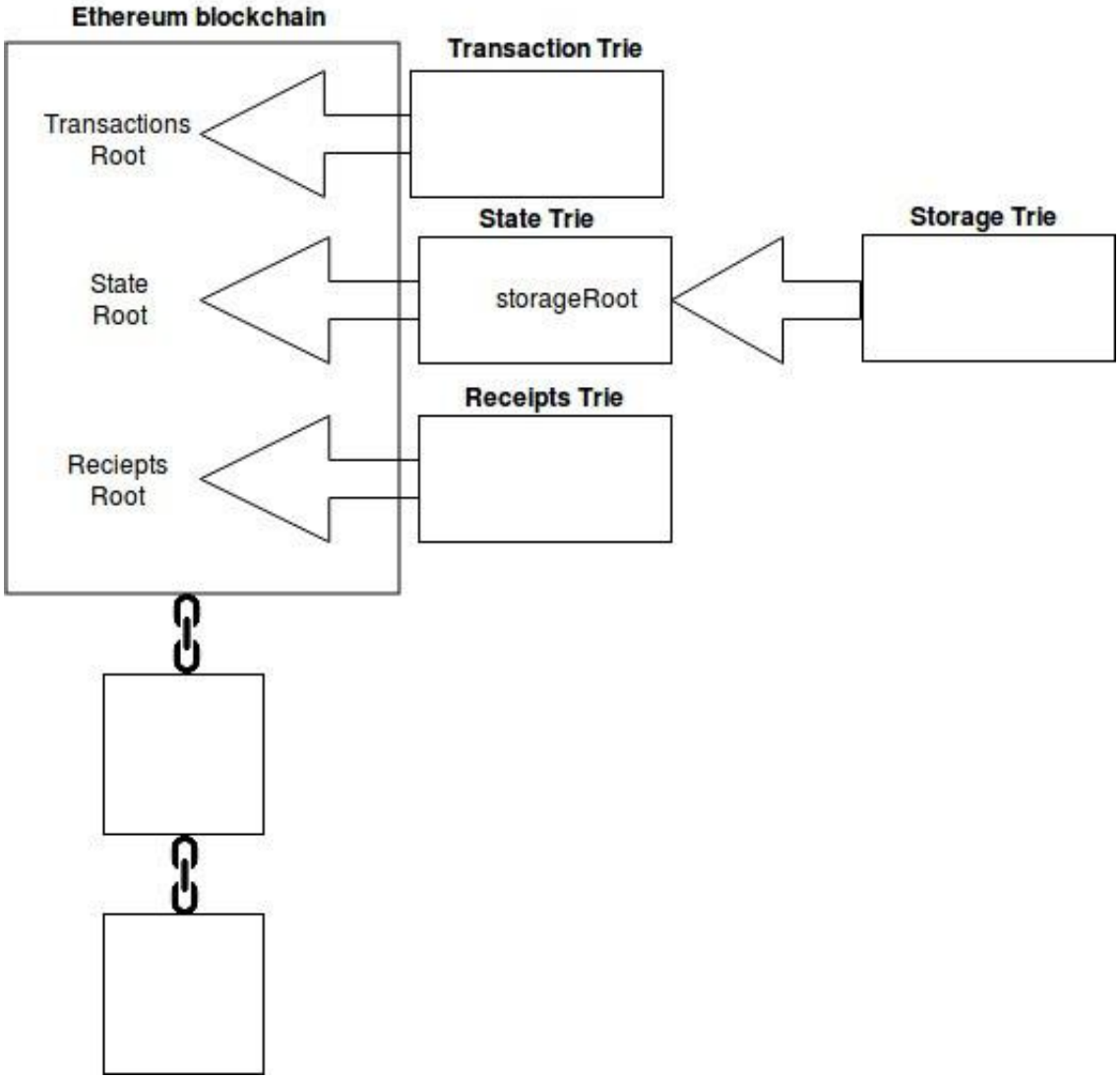
此文我们会深入讨论以太坊数据存储层。我们会介绍区块链“状态”的概念。同时也会讨论Patricia前缀树结构背后的理论，使用谷歌的leveldb数据库演示以太坊前缀树的具体实现。

在存储层中，我们存储的是什么？



其次，在最基本的层面，比特币没有包含用户账户余额。通过比特币，用户可以简单地持有私钥，在任何时间点都可以进行一个或者多个UTXO。数字钱包看起来像是让比特币区块链能够自动地存储和管理用户账户余额，其实不是这样。



也许你也注意到了，从上面的图表中，存储树的根节点哈希（所有的智能合约数据存储在其中）其实都是指向状态树的，从而指向区块链。接下来，我们会讨论更多细节。

以太坊中有两种不同的数据类型：永久数据和暂时数据。永久数据的例子就是转账。一旦转账确认，就会在区块链中记录；然后就再也不可以更改。暂时数据的例子就是特定以太坊账户地址的余额。账户的余额就会存储在状态树中，并且当有特定账户转账的时候，就会改变。永久数据是有意义的，就好像挖矿转账，暂时数据，就例如账户余额，应该被分开存储。以太坊会使用数据树结构来管理数据。

以太坊的数据记录就好像在银行。类似使用ATM机器和存储卡。银行会追踪每个借记卡来确保在在完成转账之前，有足够的余额。

UTXO和账户方案之间的对比

UTXO模型的好处：

• 扩容性 –
因为可以同时处理多个UTXO，所以能够完成同步转账并且鼓励扩容创新。

• 隐私 – 尽管比特币并是不完全的匿名系统，但是UTXO可以提供更高层次的隐私性，只要用户使用为每个转账提供新的地址。如果有需要提高隐私性，更多复杂的结构，例如环形结构，也可以考虑使用。

账户/余额模式的好处：

• 简单化- 以太坊使用的模型，可以帮助开发者来进行复杂的智能合约，特别是需要状态信息或者包含多方的。

举例来说，追踪状态的智能合约，并且基于它处理不同的任务。UTXO的无状态模型会让转账包含状态信息，而且这也不必要地符合合约的设计。

• 效率- 除了简单化，账户/余额模型更加有效，因为每个转账都只需要来验证发出金额的账户是否有足够的余额来支付转账。

账户/余额模型的缺陷是双花攻击。可以增加递增的随机数来抵消这种类型的攻击。在以太坊中，每个账户都有空开可见的随机数，每次进行转账的时候，随机数就会增加。这可以帮助防止同样的转账会进行两次。（注意，这个随机数并不是工作量证明中的随机数，这是个随机数字）

和大多数计算机架构相同，这两个模型都有自己的好处和坏处。有些区块链，例如超级账本，也应用了UTXO，因为他们从比特币区块链中获得创新。接下来，我们来看看更多的基于这两个模型的技术。

以太坊中的数据树结构是什么？

我们来深入看看，状态，存储和转账的树结构是怎样的。

状态前缀树- 是唯一和独特的。

在以太坊中，只有唯一的网络状态前缀树。

这个网络状态前缀树会实时更新。

网络状态前缀树包含秘钥和每个账户的价值对，这些是在以太坊网络上。

秘钥是单个160字节的认证器（以太坊账户的地址）。

网络状态前缀树的“数值”是通过对以太坊账户以下账户细节的编译得出的：

-随机数

-余额

-storageRoot

-codeHash

状态前缀树的根节点（某个时间点，整个网络状态前缀树的哈希）是用来保证状态前缀树的安全和唯一；网络状态前缀树根节点是基于整个内部网络状态前缀树数据进行加密。

存储前缀树，智能合约数据存储的地方

存储前缀树是智能合约数据存储的地方。每个以太坊账户都有自己的存储前缀树。存储前缀树根节点是256字节的哈希值，作为storageRoot的数值存储在网络状态前缀树。

分析以太坊数据库

在以太坊区块链中，有很多的MPT（Merkle Patricia Tries）（代表每个区块）：

- 状态前缀树
- 存储前缀树
- 转账前缀树
- 回执前缀树

为了得到某个特定区块中的MPT，我们需要获得它的跟哈希，作为参考。以下的命令可以让我们获得状态，转账和创世区块中回执的根哈希。