Bitcoin 开发者指南

这份开发者指南并不是一份说明书，它的目的是为你了解比特币和开始构建一个比特币为基础的应用程序提供一些你必须了解的信息。为了更好的使用这份文档，你需要从源代码或者预编译可执行文件中安装当前最新版本的bitcoin core。

关于比特币开发中的疑问最好到比特币开发社区去提问。关于[bitcoin.org](http://bitcoin.org)上的这篇文档中的错误和建议可以提交问题或者发布到bitcoin-documentation 的邮件列表。

在下文中有一些字符串被缩短或者覆盖：

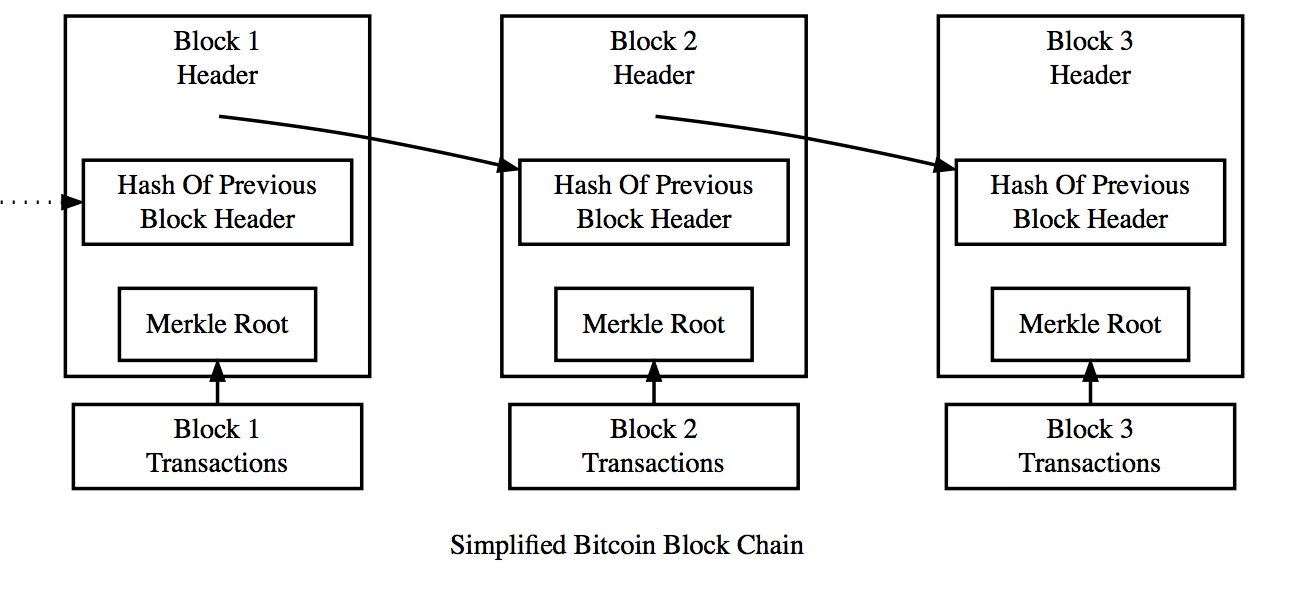
[…]表示额外的数据被删除，一行以反斜杠\结尾表示跟下一行是在同一行。如果你将鼠标指针放到段落上方，交叉引用链接会显示为蓝色。如果你将鼠标指针放到交叉引用链接上方，提示框中将会显示这条术语的简短定义。

区块链

区块链为比特币提供了一份按时间排序的公共总账。这个系统被用来防止双花和修改之前的交易记录。

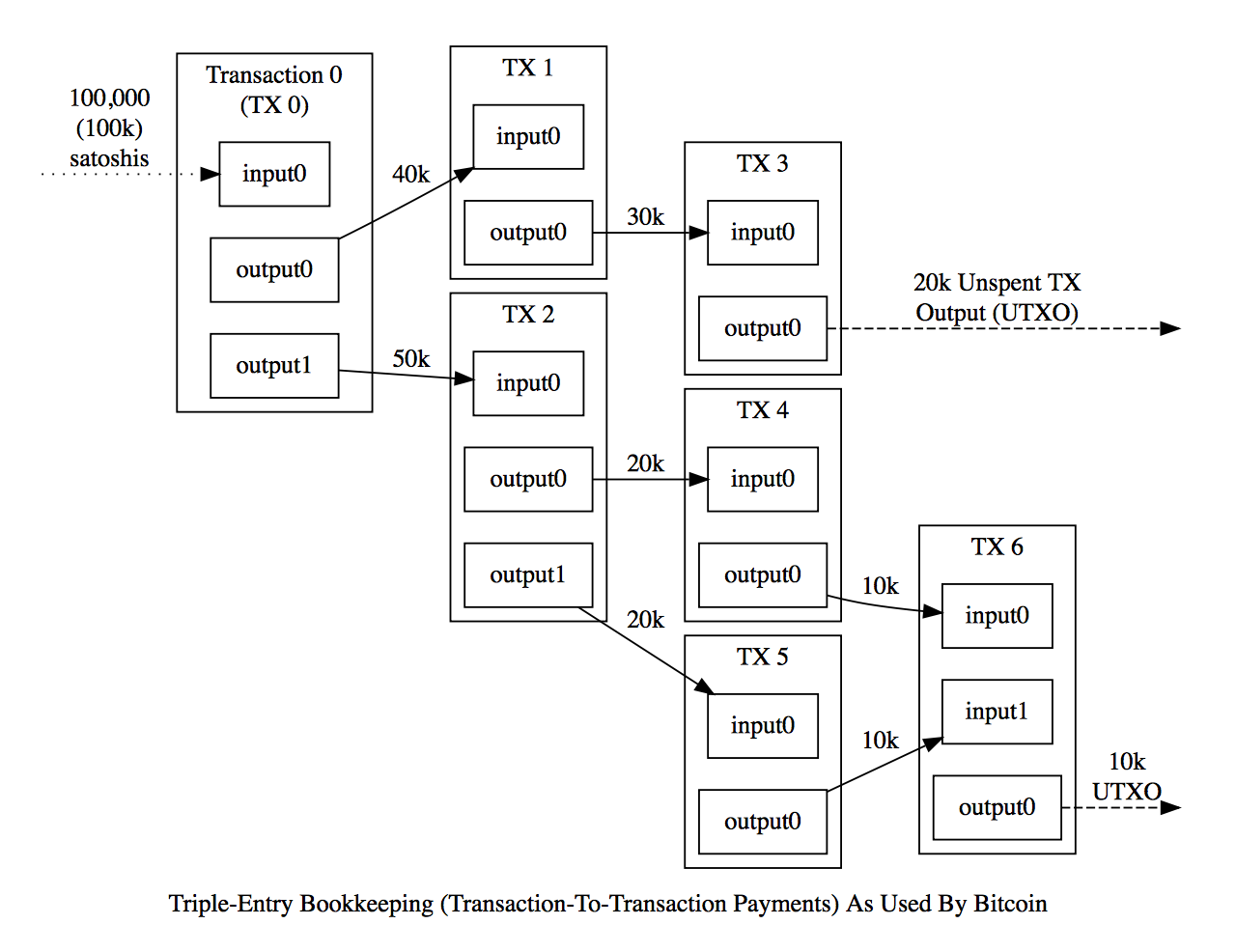
比特币网络中每个节点都独立的储存了一个经过节点验证过的区块所组成的区块链。当一些节点在它们的区块链中包含的所有区块都相同时，这些节点被称作达成共识。这些节点为了维持共识所遵守的有效性规则被称为共识规则。这个章节将会描述许多倍比特币core所使用的共识规则。

区块链概述



上面的这个插图展示了一个区块链的简化版本。一个或多个新的交易块被收集进区块中的交易数据部分。每一个交易的拷贝都会被哈希，哈希后配对，然后再哈希再配对，知道剩下一个哈希值，这个值就是默克尔树(merkle tree)的默克尔根(merkle root)。

默克尔树储存在区块头。每个区块都会保存前一个区块头的哈希值，使得区块之间相互链起来。这样确保了一个交易不会被修改除非修改记录这个交易的区块和它后面跟随的所有区块。

交易记录也会相互链接起来。比特币钱包这个软件给人的印象是聪在钱包之间消费，但是比特币实际是在交易之间流动。每次交易的花费都是从之前一个或多个交易获取的，所以一个交易的输入就是前一个交易的输出。

单个交易可以创建多个输出，就像一个投递到多个地址的箱子，但是在区块链中每一个输出只能被用作一次输入。任何后来的引用都禁止双花－－－一种把相同的比特币消费两次的尝试。

输出和交易标识绑定。交易标识就是单个交易的哈希值。

因为每个交易的输出职能被消费一次，在区块链中所包含的所有交易的输出都能被分成未花费的交易输出（UTXOs）和已花费的交易输出。对于一次有效的支付来说，必须用未花费的输出作为输入。

忽略币基交易，如果交易的输出超过了它的输入，那么交易将被废弃，但是如果输入超过输出，那么任意金额的比特币可能被比特币的矿工——创造包含交易的区块的人，作为交易费用扣除。举个例子，在上面的图例中，每次交易的花费都比它从币基的输入少10000聪，实际上就是支付了10000聪的交易费。