收款人确认单据签署人

老李拿到这个单子后，需要确认这个单子确实是来自“HIJKLMN”这个人（也就是老张）签署的，老李拿出印章扫描器扫一下章，如果液晶屏显示出的字符和付款人字符是一致的（这里是“HIJKLMN”），就可以确认单子确实是付款人签署的。

这是因为根据保密印章的机制，没有其他人可以伪造印章，任何一个人只要扫描一下印章，都可以确认单子的付款人和盖章人是否一致。

收款人确认付款人余额

通过保密印章，收款人虽然可以确认付款人确实签署了这份单子，但是无法自行确认付款人是否有足够的余额支付。

之前的中央虚拟货币系统中，二狗子负责检查付款人的余额，并通知收款人交易是否有效，现在把二狗子开了，谁来负责记账和确认每笔交易的有效性呢？

中本聪设计的这个系统是分布式货币系统，不依赖任何中央人物，所以不会有一个或少数几个人负责这件事，最终承担这份工作的是之前所提到的矿工组织。

任何使用比特币进行交易的村民都依赖矿工组织的工作才能完成交易。

矿工的工作

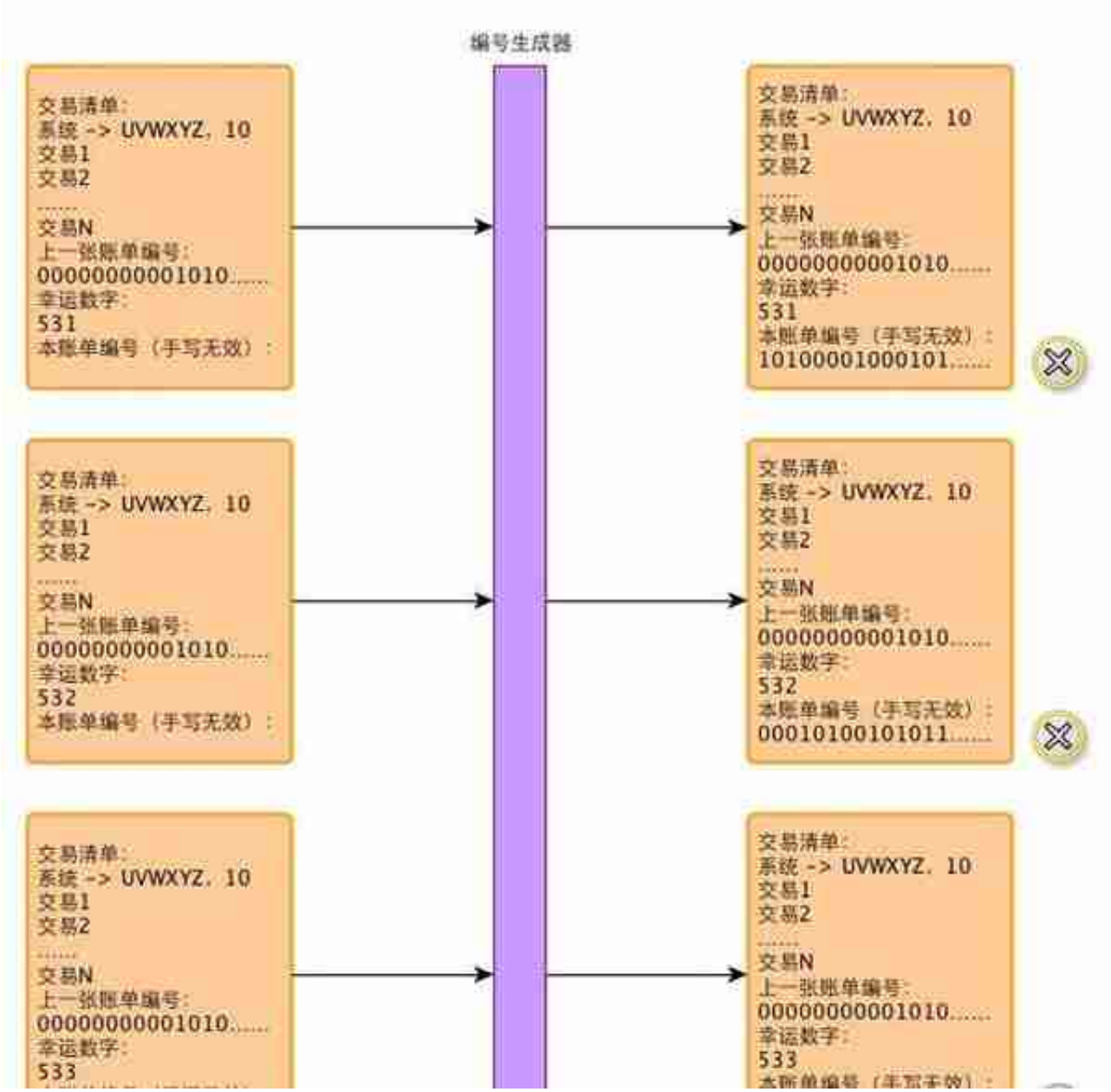
矿工的工作是整个系统的核心，也是最复杂性最高的地方。

矿工的工具

俗话说，工欲善其事，必先利其器。比特币矿工虽然不用铁撅、铁锹和探照灯等工具，不过也要有一些必备的东西。

初始账簿。
每个组首先自己复制一份初始账簿，初始账簿只有一页，记录了系统的第一次赠送。

空账簿纸。
每个小组有若干账簿纸，每一页纸上仅有账簿结构，没有填内容，具体内容的书写规则后面讲述。下面是一张空账簿纸的样子，各个字段的意义后面会说到。



在幸运数字尝试到“533”时，系统生成了一页有效账簿。

确认账簿

当某挖矿小组幸运的生成了一张有意义的账簿，为了得到奖励，必须立刻请其它小组确认自己的工作。前面说过，当前村里有7个挖矿组，所以这个小组必须将有效账簿纸誊抄6份快马加鞭送到其他6个小组请求确认。

中本聪规定，当某个小组接到其他小组送来的账簿纸时，必须立即停下手里的挖矿工作进行账簿确认。

需要确认的信息有三个：

账簿的编号有效

账簿的前一页账簿有效

交易清单有效

首先看第一个，这个确认比较简单。只要将送来的账簿纸放入编码生成器进行验证，如果验证通过，则编号有效。

第二部分需要将账簿页上的“上一页账簿纸编号”和这个小组目前保存的有效账簿最后一页编号比对，如果相同则确认，如果不同，需要顺着已有账簿向前比对，直到找到这个编号的页。如果没有找到指定的“上一页账簿纸编号”对应的页，这个小组会将此页丢掉。不予确认。

注意，由上面的机制可以保证，如果各个小组手里的账簿纸是相同的，那么他们都能按同样的顺序装订成相同的账簿。

因为后面一张纸的编号总是依赖前面的纸的编号，编码生成器的机制保证了所有合法账簿纸的相对先后顺序在每个小组那里都是相同的（可能会有分支，但不会出现环，后面细讲）。

参考：

Bitcoin: A Peer-to-Peer Electronic Cash System

https://bitcoin.it

云风的BLOG: Bitcoin 的基本原理

易懂的比特币工作机理详解

特别声明：

币圈大白社的所有文字与信息，均不构成任何投资引导意见！

经过本文普及，对于数字货币和区块链你有略知一二吗？欢迎在下方留言参与讨论。