第七讲 挖矿

前言

通过前一个单元，我们已经知道如何利用公钥密码交易数字化问题，那么数字货币化问题就还剩下记账去中心化问题没有解决。

数字货币运行在一个p2p网络中，所有用户都是这个网络中的节点，地位都是均等的。人人都可以创建、发送和转发交易信息，因此会有很多交易信息在这个网络中流转。

可是，没有中心节点，该由谁来把交易信息记录下来呢?

这个问题暂且放下，我们稍后再考虑。假设有一个好心人，他自愿把所有收到的合法交易记录下来，形成一个账本，并向全网公开。

账本可信问题

可是，其它用户凭什么相信他记录的账目没有被他篡改过呢?

比如，他会不会把他自己曾经转出的一笔交易从账本上删除呢?

还记得有什么密码学工具是用来保护消息有没有被篡改的吗?

对！哈希函数!

解决方案1

记账人自证清白的提议

这个好心人为了自证清白，就在账本的最后附上账本的哈希值，并向全网公开。

这样一来，其它用户就可以通过检查账本的哈希值和记账人公开的哈希值是否一致来检验还他是否篡改账本了?

存在的问题

你肯定已经想到了，这个记账人又不是傻子，他如果要篡改账本，那么他一定会连同哈希值一起改掉。我怎么知道哈希值有没有被你一起改掉。

问题分析

要自证**账本**没有被篡改，就需要自证**账本的哈希值**没有被篡改；为了自证**账本哈希值**没有被篡改，就需要自证**账本的哈希值的哈希值**没有被篡改；为了自证**账本的哈希值的哈希值**没有被篡改，就需要自证**账本的哈希值的哈希值的哈希值**没有被篡改……

解决方案2

记账人自证清白的提议

这个记账的好心人又想出了一种自证清白的方案。

那就是把账本分成若干块，分别计算每一块的哈希值，并将前一块的哈希值记录下下一个区块中。这些块就这么连接起来，可不就是区块链吗？

记账人的言下之意是，你看这些哈希值我都没改过吧？我只要篡改任何一笔交易，那么他所在的区块的哈希值就会改变，就会和下一个区块中所记录的哈希值不一致。

记账人这么有诚意，我们差点就可以相信它了。

存在的问题

不对啊，虽然篡改交易会导致块的哈希值变化，但是他还可以篡改下一个区块中所记录的哈希值啊！当然，这样会引起连锁反应，如果这个交易所在的区块之后有10个区块，那么就要重新计算11次哈希值。可是，毕竟哈希函数有一个特性是——运算高效，重新计算11次哈希值，并不是什么难事，很快就可以完成。

问题分析

其实到这里，你或许已经察觉到什么了，我们之所以怀疑记账人，根本原因是记账太容易了，记账容易就意味着改账也容易。

那么怎么才能让记账变难呢？

> *你一定扔过筛子，只要筛子是标准的，筛子落地后的点数为1、2、3、4、5或6的概率就是相同的，都是$\frac{1}{6}$。如果有人要求你扔出的筛子点数必须小于3，也就是说点数必须为1或2，那么你每扔出一次筛子能够满足要求的概率是$\frac{1}{6}+\frac{1}{6}=\frac{1}{3}$。按照概率期望，也就是说平均需要扔3次筛子才能第一次达到要求。*

其实，由于密码学哈希函数具有抗碰撞性，所以每计算一个消息的哈希值就也像是扔一次筛子。只不过这个筛子是很多很多面的。例如SHA256哈希值长度是256位，所以计算一个消息的SHA256哈希值就像是扔一个2的256次幂个面的筛子。

解决方案3

普通用户给记账人设计的难题

根据这个原理，**我们可以集体给记账人出一个难题，比如要求所有区块的哈希值都必须小于某个数字n。否则账本就不合法。**

一个区块的哈希值完全是由这个区块里记录的交易信息决定的，那么区块的哈希值怎么可能那么巧就是小于n的呢。这不是让记账人完成一个不可能完成的任务吗？

为了让这个任务能完成，我们允许记账人在每个区块记录的交易信息之外，额外加入一条数据，这条数据名字叫Nonce。

这个Nonce正是区块链技术的精华所在！

这样一来，记账人就可以填入恰当的Nonce值让区块的哈希值合法。

可是，这样的Nonce值上哪找去？

由于密码学哈希函数具有单向性，记账人没有办法根据哈希值小于n的要求逆推出一个合法的Nonce值。记账人只能随机尝试不同的Nonce值才能让区块的哈希值达到合法要求。

这就像是记账人一次又一次的掷筛子，直到筛子的点数达到用户设定的要求。

按照难题要求，填入一个随机的Nonce值恰好能让区块哈希值小于n的概率是$\frac{n}{2^{256}}=\frac{1}{\frac{2^{256}}{n}}$，也就是说平均情况下，需要尝试$\frac{2^{256}}{n}$个随机的Nonce值，才能使区块的哈希值合法。

由于密码学哈希函数具有运算高效的特性，所以尝试一次Nonce值并不需要花费多长时间，但是如果n设置的比较小，那么尝试$\frac{2^{256}}{n}$个随机的Nonce值显然是一个巨大的工作量。

效果分析

> *坏消息是：记账变得困难了。*
>
> *好消息是：篡改账目也变得困难了。*

记账人如果再要篡改某一笔交易，不仅这个区块的哈希值会变得不合法（当然，这并不是绝对的。），而且由于下一个区块还记录着上一个区块的哈希值。为了保持一致，还需要同步的篡改下一个区块中所记录的上一个区块的哈希值，这样一来下一个区块的哈希值也会变得不合法（当然，这也不是绝对的）。为了让整个区块链账本合法，记账人需要为此后的所有区块都找到一个恰当的Nonce值。找到一个Nonce都要付出巨大的工作量，更何况是找多个Nonce值。那肯定是不可能在短时间内完成的工作量。

所以，只要记账人能做到我们对每个区块的哈希值的要求（小于n），我们就可以放心大胆的相信他的账本是没有被篡改过的。

在这种机制下， 记账人付出了巨大的工作量来向我们证明他的账本没有被篡改，所以这种机制就叫做**工作量证明，简称POW（Proof of Work）**。

计算出Nonce值的过程被称为**挖矿**。

完成这个操作的人当然就被称做**矿工**。

谁来记账的问题

通过工作量证明，账本可信的问题算是解决了，可这个解决方案是建立在有个好心人自愿记账的假设下的。在这个方案中，要完成工作量证明才能记账，谁会愿意付出这么多的计算资源来无偿奉献呢？

所以，数字货币中都会设计一套奖励机制，谁记账，就给谁奖励。

比如，在比特币中，谁通过挖矿记录了下一个区块就会获得一定数量的比特币奖励。

激励的来源

这些奖励的比特币从哪来呢？有两个来源，一是无中生有，二是交易手续费

无中生有

什么是无中生有呢？其实这就是比特币的发币机制。矿工每记录一个区块，都可以在这个区块中额外记录一笔转出账户为空，转入账户是自己账户，转账金额为50比特币的交易。如此一来，比特币体系中就多了50个比特币流通。

可是随着区块链的增长，流通的比特币不就越来越多了吗？这不会通货膨胀吗？中本聪也考虑了这一点，所以在他的设计中，每增长21万个区块，奖励就减半。如此一来，比特币的总量就会固定在2100万个。

交易手续费

第二个奖励来源是交易的手续费。有的用户在创建转账交易时，愿意额外付出一些交易费，那么他就会把交易费也记录在交易信息中。而矿工在记录下一个区块时，就会优先收集哪些有交易费的交易打包成区块。

小结

本节课，我们通过记账人和普通用户之间的博弈过程，学习了区块链、Nonce、工作量证明、挖矿的基本原理，这里综合运用了哈希函数的运算高效、单向性和抗碰撞性；

我们还了解了区块链中是如何通过奖励机制来促进用户主动记账的。

可是你肯定还会冒出好多问题，既然记账有奖励，就可能会有很多人一起抢着记账，奖励该给谁呢？他们记的账本不一样怎么办？下节课，我们继续为您讲述。