区块链记账原理

2017-10-25 | 2018-07-31 | 比特币

区块链(1.0)是一个基于密码学安全的分布式账本，是一个方便验证，不可篡改的账本。
通常认为与智能合约相结合的区块链为区块链2.0, 如以太坊是典型的区块链2.0
很多人只了解过比特币，不知道区块链，比特币实际是一个使用了区块链技术的应用，只是比特币当前太热，把区块链技术的光芒给掩盖了。区块链才是未来，期望各位开发人员少关心币价，多关心技术。
本文将讲解区块链1.0技术是如何实现的。

哈希函数

在讲区块链记账之前，先说明一下哈希函数。
哈希函数：Hash(原始信息) = 摘要信息
原始信息可以是任意的信息, hash之后会得到一个简短的摘要信息

哈希函数有几个特点:

- 同样的原始信息用同一个哈希函数总能得到相同的摘要信息
- 原始信息任何微小的变化都会哈希出面目全非的摘要信息
- 从摘要信息无法逆向推算出原始信息

举例说明:
Hash(张三借给李四100万，利息1%，1年后还本息 .....) = AC4635D34DEF
账本上记录了AC4635D34DEF这样一条记录。

可以看出哈希函数有4个作用:

- 简化信息
  很好理解，哈希后的信息变短了。
- 标识信息
  可以使用AC4635D34DEF来标识原始信息，摘要信息也称为原始信息的id。
- 隐匿信息
  账本是AC4635D34DEF这样一条记录，原始信息被隐匿。
- 验证信息
  假如李四在还款时欺骗说，张三只借给李四10万，双方可以用AC4635D34DEF来验证原始信息

哈希函数的这4个作用在区块链技术里有广泛的运用。
（哈希函数是一组函数或算法，以后会发文章专门介绍哈希）

区块链记账方法

假设有一个账页序号为0的账页交易记录如下:

账号	入账	出账	余额	备注说明

账号	入账	出账	余额	备注说明
王二	100		190	收到xxx货款
张三		100	30	xxxx
李四	120	90	170	xxxx

记账时间为：2017-10-22 10:22:02

区块链在记账是会把账页信息（包含序号、记账时间、交易记录）作为原始信息进行Hash, 得到一个Hash值，如：787635ACD, 用函数表示为：

```
1    Hash(序号0、记账时间、交易记录) = 787635ACD
```

账页信息和Hash值组合在一起就构成了第一个区块。

> 比特币系统里约10分钟记一次账，即每个区块生成时间大概间隔10分钟

在记第2个账页的时候，会把上一个块的Hash值和当前的账页信息一起作为原始信息进行Hash,即：

```
1    Hash(上一个Hash值、序号1、记账时间、交易记录) = 456635BCD
```

这样第2个区块不仅包含了本账页信息，还间接的包含了第一个区块的信息。依次按照此方法继续记账，则最新的区块总是间接包含了所有之前的账页信息。

所有这些区块组合起来就形成了区块链，这样的区块链就构成了一个便于验证（只要验证最后一个区块的Hash值就相当于验证了整个账本），不可更改（任何一个交易信息的更改，会让所有之后的区块的Hash值发生变化，这样在验证时就无法通过）的总账本。