比特币所有权及隐私问题-非对称加密应用

2017-11-02 | 2018-03-17 | 比特币

比特币系统是如何确定某个账户的比特币是属于谁的？谁可以支付这个账户比特币？
如果你对这个问题还不是很明白，那就一起来看看吧。

银行系统

我们先来回顾下现实的银行系统：

1. 首先我们需要把我们的个人信息（如身份证）给银行，银行给我们开立相对应的账户，银行在开户的时候确立了对账户的所有权。
2. 进行支付的时候，银行对交易双方完成转账（银行在开户的时候已经知道我们对应的账户）。

同时银行会对账户信息进行保密（这点其实不能保证）。

匿名账本

那么比特币如何在没有第三方银行的参与下，在确保隐私的同时如何确定账户所有权的呢？

实际上比特币的账户是用地址来表示，账本上不显示个人信息，转账是把比特币从一个地址转移到另一个地址。
转账记录如这样：

```
{
    "付款地址": "2A39CBa2390FDe"
    "收款地址": "AAC9CBa239aFcc"
    "金额": "0.2btc"
}
```

接下来问题就变为了 谁有权用某个地址进行付款。

> 支付和所有权 实际是同一个问题，如果此比特币只有我可以用来支付，那么说明我拥有所有权

地址与私钥

比特币的解决方案是，谁拥有某个地址的私钥(如果完全没有加密概念的人，可以简单的把私钥当作密码)，谁就能用这个地址进行支付。（所以私钥一定保管好，如果私钥泄漏，比特币就可能丢失）

比特币地址和私钥是一个非对称的关系，私钥经过一系列运算（其中有两次Hash）之后，可以得到地址, 但是无法从地址反推得到私钥。

```
地址:  2A39CBa2390FDe
私钥:  sdgHsdniNIhdsgaKIhkgnakgaihNKHIskdgal

Hash(Hash(fun(sdgHsdniNIhdsgaKIhkgnakgaihNKHIskdgal)))  -> 2A39CBa2390FDe
```

> 银行系统银行账号和密码是完全独立的，无法互相推导，转出时需要同时验证账号和密码

还是上面交易的例子：

```
{
    "付款地址": "2A39CBa2390FDe",
    "收款地址": "AAC9CBa239aFcc",
    "金额": "0.2btc"
}
```

只有拥有地址2A39CBa2390FDe的私钥才能进行支付。

非对称加密技术

这个时候问题就变为了，如何证明你拥有某个地址的私钥（在不泄漏私钥的情况下）。

对交易信息进行签名

实际在签名之前，会先对交易信息进行Hash运算得到摘要信息，然后对摘要信息进行签名。过程大概是这样：
1.对交易进行hash， 得到一个摘要信息（Hash值）

```
hash('
    {"付款地址": "2A39CBa2390FDe",
    "收款地址": "AAC9CBa239aFcc",
    "金额": "0.2btc"
    }') -> 8aDB23CDEA6
```

2.用私钥对交易摘要进行签名（付款方在安全的环境下进行，以避免私钥泄密），用代码表示大概是这样。

```
#参数1为交易摘要
#参数2为私钥
#返回签名信息
sign("8aDB23CDEA6", "J78sknJhidhLIqdngalket") -> "3cdferdadgadg"
```

广播

在签名运算之后，付款节点就开始在全网进行广播：我支付了0.2btc到AAC9CBa239aFcc,签名信息是3cdferdadgadg，你们来确认一下吧。

广播过程实际上是发信息到相连的其它节点，其它节点在验证通过后再转发到与之相连的节点，这样的扩散过程。

广播的信息包含了交易原始信息和签名信息

验证

其它节点在收到广播信息之后，会验证签名信息是不是付款方用私钥对交易原始信息签名产生的，如果验证通过说明确实是付款方本人发出的交易，说明交易有效，才会记录到账本中去。

（实际还会验证付款账号有没有足够的余额，我们暂时忽略这点）
验证过程实际是签名过程的逆运算，用代码表示大概过程是这样的：

```
#参数1为签名信息
#参数2为付款方地址
#返回交易摘要
verify("3cdferdadgadg", "2A39CBa2390FDe") -> "8aDB23CDEA6"
```

如果验证输出的信息和原始交易信息的hash一致，则验证通过，记录账本，用代码表示大概是这样：

```
if(verify("3cdferdadgadg", "2A39CBa2390FDe")
    == hash('{"付款地址": "2A39CBa2390FDe",
              "收款地址": "AAC9CBa239aFcc",
              "金额": "0.2btc"}')) :
    # □□写入账本
    # 广播
else:
   # donothing
```

大家可以理解为付款地址为公钥，签名过程即为用私钥对交易摘要的加密过程，验证过程为用公钥解密的过程(为方便大家理解，严格来讲是不准确的)。

补充说明

上面为了更好的理解，我对一些信息进行了简化。

比特币系统使用了椭圆曲线签名算法，算法的私钥由32个字节随机数组成，通过私钥可以计算出公钥，公钥经过一序列哈希算法和编码算法得到比特币地址，地址也可以理解为公钥的摘要。