15 以太坊的账户

以太坊系统中的账户模式。比特币系统是transaction based manner，系统中并没有记录每个账户的资产。只能通过UTXO来推算。这种模式的好处是隐私保护比较好，你有多少钱可能连自己都说不清楚。这样的问题就是使用上比较别扭。比如说A给B十个比特币，A要说明这10个币的来源。这和平时去银行的体验不太一样，去银行是存钱的时候要说明钱是从哪来的，而不是花的时候。比特币另外一个比较别扭的是，一笔交易收到币第二次的时候必须一次性花出去。比如说A->B(10BTC)，现在B要给C 3个比特币，如果直接写B->C(3BTC)，剩下的7个BTC直接当成交易费。所以剩下的BTC必须再转给自己的另外一个账户。日常生活中我们是不需要进行这样的操作的。

以太坊系统采用的是基于账户的模型。这和日常的银行账户是非常相似的。系统里要写明每个账户里的以太币的余额。交易的时候A -> B(10ETH)，只需要验证A的账户上确实有这么多钱就行了。不需要说明具体是把哪10个币转给B，也就是不需要说明币的来源。转的时候也不需要一次性全花出去，因为会储存余额。而且现在也不需要哈希指针指向币的来源。

比特币的主要问题就是double spending attack。但是以太坊的机制对于double spending attack有天然的防护。花几次就扣几次，所以多花多扣，double spending就没有好处了。这么看以太坊全是好处，那么以太坊有什么弱点呢？如果有人篡改自己的账户余额，怎么办？发布交易的时候其实不需要说明自己的账户余额，而是全节点中的状态树来保存的，而不是自己修改的。除非将所有的全节点中存储的余额信息都改了。

Replay attack。重放攻击。比如说现在A->B(10ETH)，然后A发起交易的时候在网上广播了一遍，以为交易已经达成。这个时候如果B的恶意的，可以把这个交易在网上再广播一遍，其他的节点就会认为A又发起了一次对B的转账，从而在A的账户中扣了两次10ETH。比特币当中是不可能出现replay attack，因为是明显的double spending。防止replay attack的最简单办法就是增加一个计数器nonce，记录这个账户有史以来的所有的交易数量。然后交易的信息加上计数器需要加上A的签名。然后把这个交易发布到网上。因为有A的签名，所以计数器的信息是不能被修改的。发布到网上之后，其他的全节点的状态树里保存着这个账户的余额和计数器信息，从而可以验证这个计数器是不是对的，然后更新状态树中存储的账户的计数器。所以重放的时候就会验证不通过，就没有办法重放了。

以太坊中有两类账户，一个是叫外部账户，externally owned account。类似于比特币中的账户，产生的一个公私钥对。谁有私钥就掌握了账户的控制权。一个外部账户，也叫普通账户，里面会有余额和计数器nonce（这个名字起的不好，和比特币中的随机数起了同样的名字）。第二类账户是合约账户，smart contract account。合约账户就不一样了，不是通过公私钥对来控制的。合约账户也有balance和nonce，但是不能发起交易，以太坊中只有外部账户次啊可以发起交易。但是合约账户可以发起message来调用另外一个合约，但是不能发起交易。除此之外，合约账户还有代码code和相关的状态storage。合约账户这么被调用呢？ 你创建合约的时候会给你一个地址，调用合约的时候就是调用这个地址，调用之后合约的状态会发生改变。

为什么以太坊要创建一个新的模型？以太坊的创始人叫做Vitalik，当初创建以太坊的时候才19岁。为什么要搞一套和比特币很不一样的模型？比特币的好处就是私密性很好，可以打一枪换一个地方。所以一个人可能有好多好多账户。但是以太坊需要支持的是智能合约，就需要有比较稳定的身份，这个和日常生活当中是类似的。签合同的双方身份得是稳定的，否则会给合同的执行带来一定的困难。现在有很多人提出用智能合约来搞一些金融衍生品，就是financial derivative。所以以太坊选择了基于账户的模式，而不是比特币那样基于交易的模式。