密码学于区块链应用之我见

18308045 谷正阳

1 对区块链的理解

在传统的信用机制中，需要一个信用中间机构。如银行之于转账，支付宝、微信之于电子支付。

区块链是一种去中心化的信用机制，即不需要信用中间机构。每个人都有一份账本，都可以在账本上添加新行，然后广播出去。但是这就引出了一些问题：没有信用中间机构，如何保证没有伪造的记账；分布式的账本，如何选出有效的记账，以保证每个人的账本相同。区块链运用了密码学来解决这些问题。

2 哈希函数

哈希函数是一种可以将任意长度的消息映射成一个较短的定长输出消息的函数。一个好的哈希函数需要拥有碰撞阻力，隐蔽性，和谜题友好几个特性。

碰撞阻力是指难以找到碰撞，即对哈希函数H，对$x \neq y$，难以找到$H(x) = H(y)$。

隐蔽性保证了仅仅知道$H(x)$，没有可行的方法得到x。

谜题友好则保证了没有比随机试更好的方法得到x。

3 区块链的共识机制

3.1 数字签名

数字签名由三个算法组成：第一个算法用于生成(私钥, 公钥)对；第二个算法使用私钥加密一段消息生成数字签名；第三个算法使用公钥和消息验证数字签名是否有效。

其运作的过程是：先使用第一个算法生成(私钥, 公钥)，将私钥保管，并公开公钥。每次要广播账本，对账本运用第二个算法生成数字签名附在账本上。由于第二个算法要求消息长度有限，所以将账本先用哈希函数将账本映射成一个较短的定长输出消息即进行信息摘要。广播后，每个节点如果想验证则可用发送方公开的公钥，账本和数字签名进行验证。由于碰撞阻力，很难找到另一个账本生成相同的信息摘要，所以可以验证信息摘要来验证账本。

数字签名可以解决伪造账单的问题。由于公钥私钥对生成具有隐蔽性和谜题友好，通过公钥来获取私钥，从而仿造数字签名是需要很大时间开销的。另外数字签名生成时也引入了时间的因素，所以复制原先的数字签名也是无效的。

3.2 工作量证明

工作量证明即是通过修改区块头的随机数，然后对区块头做哈希计算，算出一个前n bits都是0的数。广播出去后，所有人可以验证该随机数的区块头运用哈希函数后是否前n个数是0。验证正确，所有人会在自己的账本上加入新的区块。新的区块会在区块头记录上一个区块的哈希值，这样区块就穿成一条链。另外有最长链机制，所有人将自己的区块接在最长链上，一段时间后短链上的交易会被撤销。因此，如果要修改其中一个区块会导致哈希值改变，从而使链断，如果想要让别人信任，需要不断地使自己的链最长。

由于谜题友好，若要解出哈希后前n bits均为0，计算平均复杂度是$O(2^n)$。时间开销很大，因而想要修改账本很困难。同时这个机制也解决了选择有效记账的问题。