Hash锁定

## Alice和Bob要交换两个链上的token。

1. Alice在A链上发送一个交易，要求有人提供s满足hash(s)=h，即可提走Alice的token
   1. 以太坊系列里，Alice把交易发到一个智能合约中，智能合约锁定Alice发送的Token，合约包括hash结果h
   2. 一般来说，合约要求对方的提币地址，即规定用Bob的地址提币。
   3. 智能合约提供一个定时交易，在Alice发送交易后2T时间内可以提走自己的Token，例如72小时
2. Bob查到Alice的交易，在B链上发送一个交易，要求有人提供s满足hash(s)=h,即可提走Bob的token。
   1. 以太坊系列里，Bob通过查询Alice的交易，可以得到Alice的金额及hash结果h，验证Alice的金额是否与约定一致。
   2. Bob发送的交易也是智能合约交易，智能合约锁定Bob发送的Token，以及hash结果h
   3. 一般来说，合约要求对方的提币地址，及规定用Alice的地址提币
   4. 智能合约提供一个短的定时交易，在Bob发送交易后T时间内可以提走自己的Token，例如36小时。
3. Alice查到B链上的Bob的交易，Alice用自己的s提取了Bob的token。
   1. Alice的s是自己第一步随机生成的，要保存到现在使用
4. Bob查到B链上Alice的交易，得到Alice的s，在A链上发送交易提取Alice的Token。
   1. Alice必须在36小时内提币，Bob有充足的时间提币。
   2. 在提币时间内，有足够的时间确认上块，如果没有上块，就再次发送提币交易。
5. 如果Alice没有提取Bob的交易，或者Bob没有发送B链的交易。
   1. Alice在72后小时提走自己的Token。
   2. Bob（如果需要）在36小时提走自己的Token。
6. 如果Alice提走Bob的交易，Bob没有提走Alice的Token，则自认倒霉。
7. 智能合约源代码可以看https://github.com/wanchain/wanchain-crosschain-contracts

标准hash锁定如下图所示：

