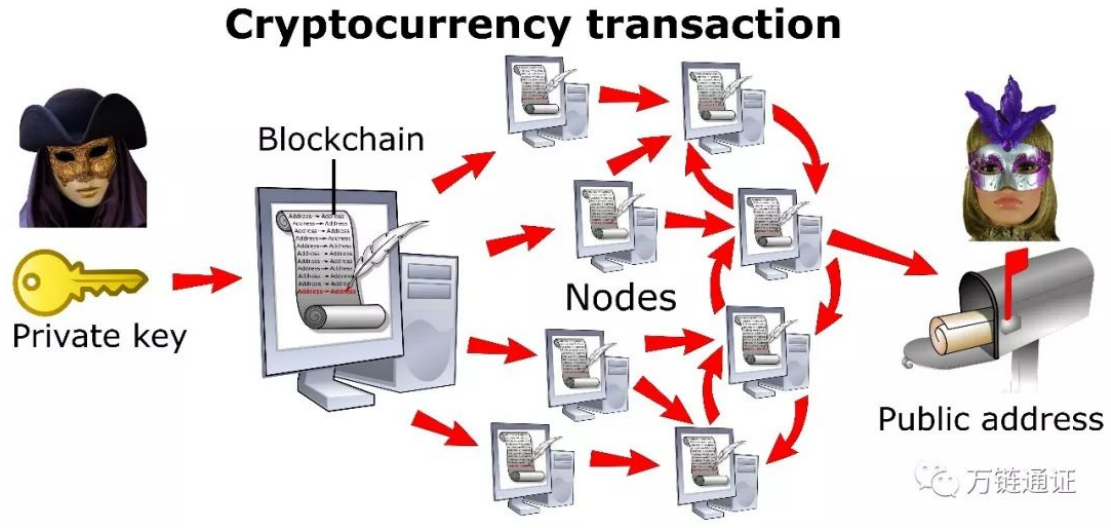
区块链的交易过程：以比特币为例

中本聪在 2008 年发表的比特币白皮书中简单描述了比特币的“交易”过程。可能由于中本聪设计比特币的主要目的是为了解决当时基于信任模式的转账的问题，原文中的 Transaction（TX）被翻译成了“交易”。这样就容易让人产生误解了，区块链入门讲解中的男女主角 Alice 和 Bob 之间暗送秋波是怎么回事？被称为区块链 2.0 的以太坊将智能合约写进区块链又是怎么回事？对照这些问题我们发现把 Transaction（TX）理解为交易似乎又不是很合适。

如果大家查一下像 Collins 或者 longman 的英文字典的解释你会发现 transaction 会有这样的解释：(in general computing)the transmission and processingof an item of data。使用谷歌翻译会显示这句话的意思是：（在一般计算中）数据项的传输和处理。把区块链中的交易过程理解成数据的传输似乎更加合理，而转账交易中的比特币只是另一种数据形式。

在区块链交易过程中，非对称加密算法扮演了一个重要的角色，区块链交易的匿名性就是由这个保证的。关于非对称加密算法的内容将在以后说明，现在只要知道：1.非对称加密算法中有一对密钥，分别为在整个网络中公开的公钥和仅自己知道的私钥；2.采用公钥加密时需要用私钥才能解密，采用私钥加密时只有公钥才能解密。下面就以比特币为例来说明区块链的交易过程。

最简单的，交易双方在协商好后进行比特币交易，随后将这笔交易广播到比特币的区块链网络上的其他节点，其他节点将对这笔交易进行验证，验证通过后矿工会将这笔交易与其他的一些交易打包成一个区块，并添加到区块链中。



当然实际的过程并不是这么简单。要进行比特币交易，你需要有一个比特币钱包。存储在比特币钱包里的不是比特币本身，而是比特币的地址。比特币的地址是一串由数字和字母组成的字符串。每个比特币的地址存有的比特币相互独立、互不影响。

你可以选择用已有的比特币地址来接受比特币，当然最好是创建一个新的比特币地址来进行交易。这样可以更好的保护自己的隐私。有趣的是在创建一个比特币

地址的时候同时产生了相应的密钥对。也就是说你可以拥有很多的比特币地址，也可以拥有很多相应的密钥对。

这时收款方将用来接收比特币的收款地址发送给付款方，付款方将这笔交易（包含付款地址、收款地址、交易额、时间戳等）使用私钥加密并广播到区块链网络中。区块链网络中的其他节点将会使用这个私钥对应的公钥来验证这是不是一笔有效的交易（即能否看到交易的内容）。

被验证的交易不会马上被矿工打包，而会被送到一个叫交易池的地方。这时矿工会选择其中的一些交易打包，然后解决一个难以解决却易于验证的密码学难题。也许这难以理解。举个例子，如果我要算出 1732 的平方根，我可以通过计算机很容易地得到结果。如果把某个平方根的整数部分去掉，取小数点后 11 到 265 位数字，需要求解出原来被开方的数，这可能就有点困难了。但是如果已经有人得到了这个数，我只要对这个数求一个平方根就可以知道这个数满不满足条件。哈希算法是一个能够把任何长度的字符串转化为一个固定长度字符串的算法，当然比上面的计算方法要复杂得多。最终需要得到一个小于特定哈希值的哈希值，这也是许多地方说的最终的哈希值要以许多 0 开头的原因。我们不能保证区块上的数据进行哈希运算之后能满足这个条件，所以加入了随机数（nonce）。将随机数加入到区块的信息中一起进行哈希运算，以得到满足条件的哈希值。最先找到这个满足条件的随机数的节点将会向整个网络中广播这条消息。同样需要被一定个数的节点验证才能生效。最终矿工会收到系统奖励的“工资”（coinbase）。正

常情况下这时你并不能确保你的交易真正生效了。需要等大约一个小时才能确保自己的交易不会被篡改或者区块链分叉导致交易失效。

就像开头所说的，区块链的交易不只是转账。在 2015 年 10 月 5 日全球第一例在区块链上记录的婚姻被提交到了区块链上。誓言被写在了文本注释字段，其中嵌入了 0.1 个比特币（当时大约 32.8 美元），这将永远被记录在区块链上。目前对于这些“交易”可能还无法做到完全免费，为普通用户提供免交易手续费的服务也将是区块链技术的努力方向之一。