区块链基础知识介绍

隆永红

一、什么是区块链?

“区块链”，可以说是时下最吸引人们眼球的概念之一。它之所以这么火爆，是因为中本聪于 2008 年发表的一篇论文“比特币：一种点对点的电子现金系统”和比特币的实用化。事实上，无论从字面上看，还是在现实生活中，区块链并非全新的概念。我们可以举一个简单的例子，张三和李四两个人在网上通过电子邮件下象棋：

首先，两个人都约好一个开局，比如重新开始的一盘棋；然后，执黑先行，比如张三，给李四发送一封邮件，“炮二平五”，李四收到后，给张三回复“马 8 进 7”，张三再给李四回复“马二进三”，李四给张三回复“马 2 进 3”，张三给李四发送“车一平二”，李四给张三回复“车 9 平 8”…… 如此往复，直到结束，他们都将拥有一个由电子邮件消息构成的序列。

顾名思义，这个邮件消息序列就是一个典型的区块链的例子，每一邮件都可以看成一个区块，代表游戏的一步。

要想使游戏能够顺利地进行，双方必须约定以下事项：1、双方都知道并认可开局的状态；2、双方都了解邮件消息序列的当前状态，记录着游戏的整体情况；3、他们可以复盘，根据邮件消息序列，他们可以重构游戏博弈的全过程。

在一个分布式系统中，没有可信中介的情况下，要想让无信任基础的双方或多方能够建立信任感，使得交易可以顺利的进行，也必须保证：1、所有参与者都认同系统的初始状态；2、他们都认同交易历史——由一系列过往交易构成的序列；3、他们认同系统的当前状态，因为它是一系列历史交易的结果。这样，区块链可以理解成：**在一个分布式系统中，并行发生但可串行化为一个由一系列交易或交易集合构成的记录序列，即，分布式账本。**

二、哈希函数与哈希链

有经验的人都知道，我们在回复邮件的时候，可以修改上一封邮件的内容，即篡改历史数据。如何保证上一封邮件不被修改？或者万一被修改了，容易被发现，从而使得我们不能否认过去发生的历史，并认可当前的状态呢？对于上面的例子，就是如何保证，在不需要裁判的情况下，我们不用担心任何一方违反三项约定。这就是时下最热门的区块链试图解决的问题，使用的就是哈希函数和哈希链的技术。

一个密码哈希函数就是具有以下性质的函数：1、以任意比特串作为输入（比如，10M 比特），可以产生一个定长的输出（比如，128 比特）；2、一个密码性质良好的哈希函数必须是防碰撞的，即，要想寻找两个

不同的比特串产生相同的定长输出是计算上不可行的。常见的密码哈希函数有 SHA256、SHA512、SHA3-256、RIPEMD-160、SM3 等。

一个哈希链就是一个记录序列，其中每个记录包含上一记录的哈希值，以及当前记录全部内容的哈希值。

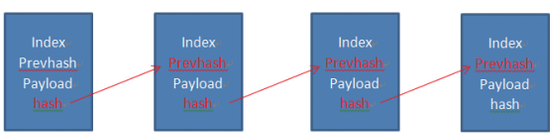

图 1：一个典型的哈希链：每个记录都包含上一记录的哈希值

如果哈希函数选择适当，意味着没有人能找到哈希值相同的两个不同的输入，意味着记录 N 是对记录 N-1 的确认，记录 N-1 是对记录 N-2 的确认，记录 N-2 是对记录 N-3 的确认……这就是哈希链的性质：每一个记录蕴含着对前面所有记录的确认，如果你改变了记录 N，意味着将改变所有后续记录 N+1、N+2……的哈希值。也就是说，一旦我们都接受了记录 N，也就已经锁定了记录 1、2、3、……、N-1 的全部内容。

区块链使用哈希链作为构件，解决历史记录或者区块内容防篡改的问题。哈希链也可用于很多其它场合：例如，在一个具有可信仲裁的系统里，可以用哈希链来限制仲裁者或中介的权力，使得 TA 不能修改历史。

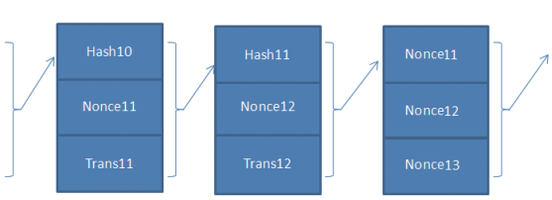

图 2. 一个典型的区块链：每一个区块包含三个主要部分，前一区块的哈希值、计数值、交易信息

三、什么是共识协议？

在区块链的形成过程中，有一个很重要的问题需要解决，那就是：怎样决定什么样的区块可以被接受为下一个区块？这时，我们没有一个可信中介，只能大家先协商一个大多数人愿意遵守的办法，然后大家按照这个办法来决定：可以把什么样的区块添加到链上？怎么添加？这个预先设计的、用来确定如何往链上添加区块的办法就是共识机制。

目前主要的共识机制有两类：一个是工作量证明，一个是许可协议。也有一些其它的共识协议设计方法，如权益证明、存储量证明等。在具体应用中，也可以是两种以上方法的融合。

所谓工作量证明，就是：你想往链上添加区块，我要你做大量的计算，并且要你证明你做过，而又不想做太多工作去检查你的证明。比特币的区块链使用的就是工作量证明，一种基于哈希函数计算的工作量证明：给定一个挑战 C 和限制 $L=2^{220}$，请你找到 N，使得 SHA256（C//N）<L，工作量的期望值是 2^{36}，每一个新的 N 都有 2^{-36} 的成功率，如果你说你成功了，我只要做一次哈希计算就可验证是否真实。

比特币设计的这种激励机制非常聪明：一是限制了新区块产生的速率、使得往链上增加非法区块的企图变得昂贵；一是当存在不一致时，提供了一种明显的方法来决定哪一个竞争链做的工作最多。但它的缺点也很明显：一是代价昂贵，为了证明所付出的工作量，需要消耗大量能源和计算资源，并且对环境造成不良影响（大量用电，只是为了让区块链保持

工作，而没有其它任何用途）；一是效率低下，工作量证明使交易速度受限，在考虑解决争议的需要时更慢。

工作量证明的替代方案之一是许可协议。许可协议基于这样的假设：我们拥有一群某种意义上可信的实体，可以一起来决定往区块链上添加区块的事情。比如，多数表决法，对有5个可信实体的情形，添加区块的合法性条件就是获得3/5以上的签名。

共识机制的设计，从某种意义上讲，就是商业模式或者业务应用模式的设计，利益分享和平衡机制的设计。比特币所设计的工作量证明实现了无中心环境下的互信机制，然而，许可协议是对中心化信任机制的妥协。

四、区块链和去中心化

人们普遍有一种误解，认为区块链就是去中心化的。其实不然，就像前面提到的，区块链与去中心化是不等同的。按照“中心”的作用程度，区块链可以分为三类：单中心、多中心、无中心。一个区块是否是去中心化的？取决于共识机制的设计。比特币的区块链是去中心化的，基于许可协议的区块链就可以认为是多中心的，基于CA的证书链信任机制多数是单中心的。值得一提的是，这里所说的多中心，其中每个中心是平等的，拥有同样的表决权，与传统信任机制中的多级中心不是一个概念。

五、区块链、比特币和数字货币

目前，人们一提到数字货币，就会想到区块链和比特币。比特币是数字货币的一种，将他们二者联系在一起是自然的，但数字货币是一个更广泛范畴的概念。我不大同意“比特币是商品，不是货币”的说法。从货币的起源来讲，无论是活的牛羊、动物毛皮、贝壳、银锭、还是黄金，曾经在充当货币的同时，他们都是商品，是一种特殊的商品，是同时具有价值尺度、储值手段和交换媒介属性的商品。比特币同样具有价值尺度、储值手段和交换媒介三重属性，虽然它的作用域远远小于主流法币，但的确已经充当了支持网络社区经济活动的所需要的货币，而且具有国际性。

虽然比特币与区块链是两个完全不同的概念，一个是充当价值尺度的交换媒介，相当于金钱；另一个是可以用来记录交易历史的账簿，人们总是将比特币和区块链联系在一起，原因也很简单：一方面，金钱与记账多数情况下是关联的，另一方面，是因为在中本聪的p2p电子现金的设计中，比特币与区块链是共生的：他用区块链记录比特币的转帐情况，也用比特币支付那些为区块链产生新的、合法区块的报酬。

区块链的用途可能不局限于比特币和数字货币，但究竟能够在哪些领域发挥作用，还将拭目以待。