【2019.11.11】新华日报·比特币：区块链技术 首个成功应用

耿 强 罗禹涵

比特币（Bitcoin），无疑是近年来最热门的话题之一。它究竟是未来货币发展的必然趋势，还是疯狂炒作的又一颗“郁金香球茎”？

首先，比特币不是任何有形的货币，它的生产和运行基于互联网，是一种开源形式的P2P（Peer to Peer）数字“货币”。不同于人类早期的因其自然属性而选择的金银货币，也不同于近100年来人们习以为常的法币（Fiat Money）——由国家法律和主权信用支撑的纸币，比特币完全诞生于现代科技互联网时代。

比特币是区块链技术的第一个成功应用。传统金融体系的交易记录都被保存在银行中心的数据库中，而区块链则是比特币的账本，任何时刻产生的比特币的所有权以及交易记录，都记录在区块链账本中。任何人只要下载了客户端，就能接收相关信息。

比特币的地址、私钥类似于个人账户与支付密码。个人拥有的比特币被锁定在个人地址上，只有运用私钥才能解锁并发往别的地址，实现交易。交易过程中会向全网发送一份账单，其他用户会对其校验，一旦通过验证，交易行为就成功了。第一个校验出这笔交易是否有效的用户，会被奖励一笔比特币。这笔奖励的比特币分为两部分：一部分是交易的手续费，这部分由转账者支付，是系统中已经存在的比特币；另一部分则是系统新生成的比特币奖励。计算机的算力越大，越有可能得到比特币奖励。所谓的“矿工”就是专门进行验证交易信息并更新记录的人。

总体而言，比特币有以下几个特性：

总量有限性，发行不会失控。比特币发行的唯一来源是记账成功后系统的基础奖励。基础奖励最开始有50个比特币，每创建21万个区块后奖励会减半，到目前为止，减半已经发生了两次，成功记账只会得到12.5个比特币。估计到2140年左右，比特币总量将达到2100万个的上限。

良好的匿名性，账户拥有者的身份不会被任何人知晓。人们可以随意地通过比特币进行转账交易，不用像银行转账那样需要核验各种身份信息，更不用与任何银行卡绑定。不过，这一特性也使得比特币在洗钱等非法交易中被大量运用，目前比特币支付的最主要用途是黑市交易和“暗网”交易等。

比特币的生产和维持耗用了大量能源。“采矿”使得每生产一个新比特币都要通过高性能计算机执行加密过程解决复杂的数学难题。由于挖矿得到的货币数量和机器的运算能力大小成正比，从概率上看，采用性能越高的硬件，在所有矿工中算力的占比越高，更易获取比特币。“矿工”们为了获得更高的收益，彼此之间在算力上进行着较量，全世界10大矿池的算力总和占据了比特币算力的75%，算力的高度集中以及维持分布式去中心化的账户需要消耗大量的能源。

比特币的价格容易大幅波动。比特币只是一堆数据，如果不与现实法币和实物挂钩，就很难确保其价格的稳定性。国家主权信用的承诺使法币在短时间内不会大幅贬值，因此人们才愿意使用法币而不是回归金银货币。与法币不同，在没有法律约束的情况下，实物所有者可以随心所欲地与比特币挂钩、脱钩，这使得比特币非常容易受非理性情绪影响，价格产生大幅度的波动。