区块链、数字货币与金融安全

文 / 李伟

区块链技术：起源、原理和特征

早在 1991 年，学者 Stuart Haber 和 W. Scott Stornetta 就提出了区块链技术（Blockchain），随后 Haber 和 Stornetta 等人又合作提出了一种重要数据结构——默克尔树（Merkle Tree），显著提升了区块链的运行效率。中本聪（Satoshi Nakamoto）于 2008 年提出并实现了比特币的区块链，此后比特币区块链发展为全球性的数字货币交易全局账本。通过解决

“双花（Double Spend）”问题，区块链技术帮助比特币成为首个不需要信任第三方的数字货币；而比特币的成功反过来又极大推动了区块链技术的应用和发展。从2014年开始，“区块链2.0”被用来指称有别于比特币区块链的新型区块链（例如以太坊（Ethereum）区块链），其特征是允许用户编写更复杂的智能合约（Smart Contract），以去中心化的方式完成各种数字资产的交易，最终实现自治的、可编程的数字社会。

本质上讲，区块链是一种分布式数据库，用来存放不断增长的交易记录，而这些记录被称为“区块”。通过使用对等网和分布式时间戳服务，区块链技术实现了自主管理，并采用共识协议完成对新区块的验证，以保证记账数据的真实性。区块链是对等网技术、密码技术、分布式存储技术以及虚拟机技术的集大成者，采用永久和可验证的方式来记录双方交易，形成一种具有开放性和分布性的可信公共账本。因此，区块链非常适合记录重要事件、医疗记录以及存证类应用，如交易管理、版权管理、身份管理等等。更重要的是，比特币区块链采用经济激励机制鼓励个体参与，催生了一种全新的数字价值共享生态系统——即通过大量分散主机自主运行共识算法来建立信任关系，不再需要信任第三方作为中介。如果用一句话来解释区块链的原理，那就是“少数服从多数”。

基于这种“共识决定一切”的原理，与传统的中心化数据库系统相比，区块链具有以下重要特征：第一，区块链上的信息不可篡改。由于采用共识算法和增量记账方式，区块链上信息不能被删除和更改，除非控制全网一半以上计算能力，而通常这几乎是不可能的；第二，区块链消除了单一故障点。通过将账本数据分布存储于全球网络中的分散节点，与中心化算法相比，区块链消除了单一故障点——黑客难以攻破所有的区块链节点，而且位于不同地点的分散节点几乎不可能全部同时出现故障；第三，区块链允许开放接入。开放接入意味着任何人都可以接入到区块链中，而无需其他人批准。这种开放性使得区块链无需防范破坏者的加入，因此也不需要对接入进行访问控制。

数字货币：产生、发展与影响

如前所述，区块链技术是随着比特币的发展而逐步得到推广应用的，因此我们无法离开数字货币来谈论区块链——区块链是技术，而数字货币则是其具体应用。2008年10月31日，中本聪在一个密码学邮件列表中首次公布了比特币的设计原理和实现方式。在2009年1月，比特币区块链网络正式开始运行，中本聪挖出了首个比特币区块（即创世块）并获得50个比特币。当时，比特币的用户多数属于酷爱科技的自由主义者，而比特币的早期交

易市场隐藏在匿名网络中，用户可以在“丝绸之路”这样的灰色交易市场上订购商品并用比特币支付。随后一些正规企业也逐步开始接受比特币，发展到现在，数字货币已经得到广泛的认可，不再被怀疑为是金融骗局或者非法工具。

到目前为止，数字货币的总市值已接近1000 亿美元，并呈现出以下发展趋势：第一，数字货币的使用趋于普及化。早在 2015 年，全球接受比特币支付的商家就已经超过十万家。与此同时，很多数字货币交易所提供全天候交易服务。另外，数字货币相关的各种衍生产品也在不断涌现，如数字货币合约交易、数字货币硬件钱包、数字货币指数基金等；第二，数字货币的类型呈现多样化。截止 2017 年 7 月，数字货币的种类已超过 900 多种。与数字货币早期阶段相比，目前比特币不再一枝独大，其他数字货币市值总和已超过比特币，这说明未来数字货币将呈现百花齐放的形态；第三，数字货币的地位正逐步走向合法化。越来越多的国家对开始支持比特币，德国、日本、加拿大、俄罗斯等重要国家都已经承认比特币的货币地位，而韩国正积极推动比特币跨境转汇服务合法化。数字货币在全球范围的合法化趋势已经成为不可逆转的潮流。

随着数字货币市值的快速增长、使用普及化以及地位合法化，以比特币为代表的数字货币已经对全球经济和社会发展产生了重要影响。一方面，数字货币作为金融科技的创新成果，将对社会和经济带来革命性变化。如果使用得当并充分发挥其积极作用，那么数字货币作为万维网技术之后最重要的技术发明之一，将极大地造福人类的生产和生活。但是另一方面，现有数字货币的匿名性和去中心化特性的确会带来一些困扰，对现有金融秩序带来不可预知的影响，甚至导致金融领域的波动和社会动荡。因此，是否完全接受数字货币在全世界范围内仍然是有争议的话题。当以比特币为代表的数字货币不断发展壮大时，正确看待其正反两方面的作用，努力化解可能的风险才是唯一正确的途径。

金融安全：加强对数字货币的技术监管

虽然比特币是技术上的发明和创新，但是这种发明完全颠覆了现有的货币发行和流通模式。比特币的去中心化思想与互联网的设计思路一脉相承，但是却与现有金融秩序背道而驰。因此，当以比特币为代表的数字货币发展到一定规模时，必然会对现在的金融行业带来不确定的风险，特别是在汇率、货币储备、货币政策、税收，投资等方面。事实上，以比特币为代表的数字货币已经成为重要的金融资产，有预测认为其市值将在未来十年内增长到万亿美元规模，届时必将对经济和金融领域造成严重冲击。同时，在全球经济一体化的大背景下，数字货币甚至有可能成为国家之间经济博弈的重要手段。因此，国家金融管理部门需要对数字货币进行全方位监管，并提早制定应对措施。

然而，由于数字货币完全由技术推动，行政手段很难达到全面监管的目的。实际上，数字货币的很多问题都需要技术手段才能解决，如以下三个实例：第一，数字货币的安全性问题。在数字货币发展史上，多次出现重大的安全问题，导致其价格大幅波动、市场动荡、甚至分裂。2011 年 6 月，由于存在安全漏洞，日本最大的比特币交易所 Mt.Gox 的比特币价格从 15 美元暴跌至 1 美分，之后更出现管理者监守自盗导致大量投资者利益受损。2011 年 8 月，比特币交易平台 MyBitcoin 遭到黑客攻击，价值超过 80 万美元的 78000 个比特币下落不明。现有的数字货币交易所仍然需要技术强化以提高安全性。第二，数字货币交易的追踪问题。比特币被人攻击的一个重要原因就是其匿名性，为洗钱、黑市交易等非法活动提供了便利。而对于此类交易行为，只有采用技术手段进行分析和追踪才能对其进行有效监管。事实上，目前多数数字货币相关案件都是通过数据分析和身份追踪破获的。第三，数字货币市场的稳定性问题。从诞生之日起，比特币价格在 9 年间增长超过 270 万倍。仅今年 5 个月上涨就超过 100%，而有时候又能一夜价格腰斩，暴涨暴跌几乎成为比特币的常态。因此，如何采用技术手段对比特币价格进行预警和干预，对于保证市场稳定性具有重要的意义。

毫无疑问，上述问题要求对数字货币的实现方法和运营机制进行技术革新，以达到有效监管的目的。为此，笔者建议国家从三个方面开展相关工作：第一，通过科技规划的方式对数字货币监管共性核心技术和基础方法的研究进行资助，如通过基金委、科技部等科研主管部门进行立项，鼓励信息领域和金融领域开展交叉合作研究，解决数字货币领域中存在的重要技术问题。第二，成立专门的工程中心，在国家层面对各种数字货币进行技术监管，实时监测市场运行、追踪异常行为，并规避可能的市场风险。第三，建议推出产业扶持政策，支持我国企业进入数字货币领域，开展相关技术、应用以及衍生品的研发，构建自主可控的数字货币生态系统，保持整个行业的稳定健康发展，应对数字货币带来的未知风险，迎接全新数字化社会的到来。

作者单位：中国科学院计算技术研究所