区块链技术的“不可能三角”及需要注意的问题研究

陈一稀

（中国人民银行杭州中心支行，浙江杭州　310001）

摘要：区块链事实上是一个技术的集合，它包含数据结构、民主网络、安全机制三层涵义。但是目前区块链技术在“高效低能”、“去中心化”以及“安全”三个方面无法同时满足，存在“不可能三角”。此外，区块链技术还存在本质上来说是“换中心”而非“去中心”、全网大量计算力并未产生真实价值、安全性的基石掌握在欧美发达国家手中以及大规模运行时抗压能力和可监管性存疑等问题。建议政府应当在区块链技术的发展中发挥重要的作用，在使用区块链技术时应根据实际应用的需要综合平衡“不可能三角”，应设法让区块链技术的计算能力解决一些有意义的实际问题，以及加强密码学等基础学科的研究，从而应对区块链技术的发展。

关键词：区块链；比特币；去中心化；分布式记账系统

中图分类号:F831　**文献标识码**:A　**文章编号**:1005-0167(2016)02-0017-05

一、技术视角下“区块链”概念辨析

“区块链”这一概念为人所广泛熟知来自基于它的一款著名应用——比特币。据统计，“区块链”已经吸引了超过10亿美元的投资，并逐渐走进了政府决策层、金融机构以及大型企业的视野。2016年1月20日，中国人民银行在北京召开数字货币研讨会，周小川行长指出需要密切关注区块链等技术发展对金融带来的影响。当前，“区块链”这个名词被广泛运用，但在使用时人们或者给它下了不同的定义，或者专门有所特指，这就造成了一定的混乱。例如，有的认为“区块链”是一种数据结构，有的认为它是一种数据库，有的定义它为一种协议，有的则用它来代表分布式记账系统。

事实上，“区块链”这个概念是多种技术的集合，其在技术角度主要解决三个问题：一是如何完整、可追溯地存储数据；二是如何构建一个可以全民参与的民主网络；三是如何确保这个民主网络安全运行。因此为了防止混淆，本文将以“区块链技术”这个更为确切的术语进行代替。

对应上述三个问题，“区块链技术”至少具备以下含义：

（一）区块链技术定义了可以表达先后顺序的数据结构

如比特币区块链技术采用了“区块+链”的数据结构，“区块”的“块身”存储数据，“区块”的“块头”存储前一个“区块”的引用，事实上形成了当前“区块”到前一“区块”的链接。从结构上看这便类似于最简单常用的数据结构——链表。

（二）区块链技术利用基于密码学的分布式协议构建民主网络

如比特币区块链技术一方面利用开源的、去中心化的P2P（Peer-to-Peer）协议构建民主网络，使得每一个节点的信息都实时广播扩散到网络中的其他节点，且每一个节点都可以存储所有完整的信息；另一方面，其又利用非对称加密技术识别信息的所有者，使得个人可以在匿名网络上证明自己的所有权。

（三）区块链技术利用“共识机制”来确保去中心化网络的安全运行

如比特币区块链技术采用“基于工作量”（Proof of Work）的共识机制，通过求解与上一区块相关的难以计算但及易验证的哈希问题，依靠大量的外部算力来确保网络的一致性、稳定性和无法篡改性。

可以说目前的比特币、纳斯达克Linq交易平台、Edgelogic钻石登记账目等都是区块链技术的具体应用，而非区块链技术本身。值得注意的是，当前大部分区块链技术集合中所涉及的单个技术，在相应的专业领域内都已是相对成熟的技术，并不存在多少创新，然而从整体上看由比特币所引发的区块链技术通过将已有技术有机结合创造了具有一定价值的基础设施，其本质是一种集成创新。

*作者感谢国家自然科学基金管理科学部2014年第3期应急管理项目《互联网金融监管研究》(项目编号:71441022)的资助。

作者简介：陈一稀（1982-），男，浙江海宁人，现供职于中国人民银行杭州中心支行。

二、“区块链”技术的“不可能三角”

在传统货币银行学中存在“不可能三角”，也称为“三元悖论”，即开放经济下一国无法同时实现货币政策独立、汇率稳定与资本自由流动，最多只能同时满足两个目标，而放弃另外一个目标。相类似，当前的区块链技术也存在“不可能三角”，即无法同时达到“高效低能”、“去中心化”、以及“安全”这三个要求，具体来看：

（一）追求“去中心化”和“安全”则无法达到“高效低能”

比特币区块链技术便是一种极致追求“去中心化”和“安全”的技术组合。

从数据结构上看，它采用拥有时间戳的“区块+链”的结构，在可追溯、防篡改上具备安全优势，也易于分布式系统中的数据同步，但是若需要对信息进行查询、验证，则涉及到对链的遍历操作，而遍历是较为低效率的查询方式。

在数据存储上，它的每一个节点都下载和存储所有数据包，利用强冗余性获得强容错、强纠错能力，使得网络可以民主自治，但同时也带来了巨大的校验成本和存储空间损耗。它并不像分布式数据库那样随着节点的增加可以通过分布式存储提高整体存储能力，而只是简单地增加副本。未来随着区块链技术所承载的内容增多，单个节点的存储空间将是个问题。

在并发处理上，比特币区块链技术最终只允许一个“矿工”获得记账权建立一个交易区块，这种机制可以有效保证一个民主网络运行的安全和稳健，但其实质上是拥有所有数据的整个“链条”在进行串行的“写”操作。相比关系数据库将数据分为若干表，仅仅根据操作涉及的数据锁定若干表或表中的记录、其他表仍能并发处理相比，比特币区块链技术的串行操作效率远低于普通数据库。

在对内容的验证上，比特币区块链让每个节点都拥有所有的内容，同时对区块内的所有内容进行哈希，这增强了民主性和安全性。但是这种整体哈希的设计思路则意味着不能以地址引用的方式存储数据，否则由于所引用地址上所存储的信息由于并未进行哈希校验而可能存在篡改。因此，比特币区块链技术缺乏高效的可扩展性，在对大型内容的处理上存在效率问题。

（二）追求“高效低能”和“安全”则无法完全实现“去中心化”

从“共识机制”角度看，为了在确保“安全”的前提下解决比特币区块链技术所采用的工作量证明方式的低效性，权益证明（Proof of Stake）、股份授权证明（Delegate Proof of Stake）等机制被采用。但是无论是基于网络权益代表的权益证明，还是利用101位受委托人通过投票实现的股份授权证明，实际上都是对“去中心化”的退让，形成了部分中心化。

同样在区块链技术的演化上，除了以比特币为代表的公有链技术外，又衍生了联盟链技术和私有链技术。联盟链技术只允许预设的节点进行记账，加入的节点都需要申请和身份验证，这种区块链技术实质上是在确保安全和效率的基础上进行的“部分去中心化”或“多中心化”的妥协。而私有链技术的区块建立则掌握在一个实体手中，且区块的读取权限可以选择性开放，它为了安全和效率已经完全演化成为一种“中心化”的技术。

（三）追求“高效低能”和“去中心化”则必须牺牲“安全”

一个极端的案例便是基于P2P（Peer-to-Peer）的视频播放软件。以往当在线观看人数增多时，基于中央服务器设计的视频服务器会因承载压力变大而速度缓慢。为了提高效率，P2P视频播放软件的设计使得一个节点在下载观看视频文件的同时也不断将数据传输给别人，每个节点不仅是下载者同时也是服务器，资源的分享形成不再依赖于中央服务器的“去中心化”模式。

同时，由于视频一秒有24帧，少量图片的局部数据损坏并不影响太多的视觉感官，但是用于数据校验而出现的图像延迟则是不可接受的。于是P2P视频播放软件牺牲了“安全”性，允许传输的数据出现少量错误。在这种去中心化的网络中，参与的节点越多，数据的传播越快，传播的效率越高。当然这对于严谨的金融业来说，数据的错误是不可接受的，安全也是金融业所首要考虑的问题。

总之，从当前的技术条件来看尚无法实现“高效低能”、“去中心化”和“安全”三者皆得的区块链技术。但是若对其一个或若干个要求进行妥协，所产生的新技术集合由于更符合实际需求，有可能它对实际应用的吸引力反而增强。

三、“区块链”技术进一步发展需要注意的问题

除了区块链技术的“不可能三角”以外，我国发展区块链技术还因当注意以下问题。

（一）区块链技术从本质上来说是“换中心”而非“去中心”

通常认为以比特币为代表的基于区块链技术的应用在运行时不需要人类来执行规则、仅仅通过数学算法来控制，因此是一种完全的“去中心”化，但从本质上看这是一种误解。比特币区块链技术虽然实现了运行时的“去中心”，但是强化了设计时的“中心化”。根据比特币的核心源代码分析，截至2015年5月14日，其50%的源代码由三位程序员编写，而前七位程序员编写的代码占据了总量的近70%。因此，比特币区块链的控制权事实上掌握在了少数程序员手中，其“中心化”的过程从运行时转换到了系统设计时。

此外，当比特币区块链的挖矿成为一种产业，或者当有国家力量参与时，其网络中“每个矿工机会均等”的假设不再成立，例如目前比特币的“矿池”和“矿场”掌握了绝大部分的算力，一台普通PC机的算力从概率上来说要200年才能挖到一次矿，已经有向中心化发展的趋势。

（二）区块链技术的大量全网计算力并未产生真实价值，与大型机、云计算等技术下的计算力输出不具备可比性

这以比特币区块链技术为甚，据统计，在2016年初比特币区块链的全网计算能力已经达到了每秒$8*10^{18}$次运算，而当前世界运行最快的计算机——美国用于核武器研发的蓝色基因超级计算机每秒的运算速度为能进行$2.8*10^{14}$次运算，从这个数据来看比特币区块链的计算能力已经是世界上最快的单台计算机的计算能力的28,000倍。

但事实上比特币区块链技术决定了每次只有一个矿工能获得记账权，那么其他矿工的计算都被浪费，这些计算力其实并未产生真正的价值。同样，比特币区块链技术的全网算力只能用于维持自身的运营，是内部的竞争式计算，并无法同云计算技术一样通过协同计算对外输出强大的计算能力。

（三）密码学是区块链技术安全性的基石，也是未来影响安全性的重要风险来源之一

一方面，密码学的安全通常定义为在当前技术水平下所加密的信息在相当长的一段时间内（如在当时计算能力条件下100年以上）无法被解密，但是随着新的数学算法的出现以及计算能力的提高，以往安全的加密信息可能在可接受的时间内被解密，那时基于此类密码学算法的区块链技术将会失去信任这一根本的基石，区块链技术的安全性就会变得越来越薄弱。

在另一方面，从我国密码学的发展水平来看其还低于国际水平，研究主要以论文为主，缺乏顶尖的研究成果，大量在实际中应用的密码学产品都来自欧美国家。从这一角度看区块链技术的核心基础其实掌握在欧美国家手中，若关乎国家命脉的核心系统构筑在区块链技术之上，则存在着不小的潜在安全风险。

（四）区块链技术处理大规模事务时其抗压能力和可监管性存疑

目前基于区块链技术的平台同真实运行的全球支付系统相比，其节点总规模数仍然较小，只处理过小部分人、零碎的事务，没有经历过全世界所有人都共同参与的大规模交易的考验，一旦将区块链技术推广到大规模交易环境下，其抗压能力仍存疑。

例如，区块链技术在节点相互通信和 维护去中心化网络时采用广播的方式通知所有节点，当节点规模增大时可能产生“广播风暴”，大量占用网络带宽导致网络性能下降，甚至网络瘫痪。

此外，区块链技术下数据和信息的完整透明一般被认为有利于监管和追踪，但是当数据规模增大时，低效的查询和挖掘会使得数据透明性的优势形同虚设，链状的数据结构和大量内容的直接记录将使得拥有反洗钱能职能的监管机构无法在可接受的时间内完成对数据的解读。

（五）要防范使用区块链技术的节点大量退出时可能出现的不稳定状态

以比特币为例，当前大量节点的参与维持了其网络的健壮性，一个重要原因是比特币自身的价格处于高位，且电费便宜，成本可以覆盖收益。中国绝大部分高计算能力的比特币矿机便分布在小水电站周边以降低成本。但是如果有一天因为成本、政治或其他因素大量结点开始退出网络，则要防范由此可能带来的区块链技术网络的不稳定性。

四、相关建议

（一）政府应当在区块链技术的发展中发挥重要的作用

任何一款涉金融的应用都需要有一个好的管理机制来保护参与者，即便是去中心化的应用，适当的监管也是必要的。况且就区块链技术而言，它更多的是“换中心”而非“去中心”，并且也正在演化出一些“多中心

化”甚至“中心化”的形态。

政府应当在了解区块链技术潜在用途、成本收益以及可能产生的伦理及社会影响的前提下，将区块链技术纳入合适的监管框架之内，例如政府可以通过立法来加强对技术代码规则的监管，从而作为区块链技术监管的切入点，或者直接作为主要节点参与“多中心化”网络的运营。

（二）在使用区块链技术时应根据实际应用的需要综合平衡“高效低能”、“去中心化”和“安全”

区块链技术类似于“地基”，比特币便是盖在这个地基上最大、最早的房子，且更多地关注了“去中心化”以及“安全”因素。未来还将有更多其他类型的应用试图“盖”在这个“地基”之上，若区块链技术的“不可能三角”仍然成立，则应当根据实际应用的需要综合平衡“高效低能”、“去中心化”和“安全”这三方面的因素，使得其系统的整体性能得到最优化。

在金融领域中，应用的“安全”是首要考虑的问题。因此在确保安全的基础上，应当综合平衡“高效低能”与“去中心化”。当然，由于区块链技术才诞生不久，未来随着越来越多的资本、人才、资源等要素源源不断地被投入到相关研究中去，区块链技术的“不可能三角”也有可能存在被攻陷的一天。

（三）应设法让区块链技术的计算能力解决一些有意义的实际问题

虽然基于哈希算法的工作量证明机制在安全性上有独特之处，但是大量计算资源被浪费，即便是计算得到的正确结果对于现实生活也意义不大。如果能将这些计算力用于解决一些现实中的“问题”，则在一定程度上能够减少其受到的“浪费资源”的诟弊。

一个例子就是验证码的有效利用。验证码的发明者当时发现全世界的网民每天要输入验证码接近2亿次，若每次花费10秒，则每天要花费50万小时，如果将这些时间有效利用，将能产生巨大的价值。于是其巧妙地设计将验证码和扫描获得的尚无法识别的文字分拆整合让用户识别，结果在短短几个月时间内，借助验证码让网民们帮忙完成了“纽约时代”130年来所有旧报纸的存档电子化工作。

（四）需要加强密码学等基础学科的研究，并加快建设信息基础设施以应对区块链技术的发展

一方面，有关部门应当联合学术界、产业界加强密码学等学科的发展战略研究，促进核心关键技术的研发以及急需产品的开发，对密码技术和网络安全相关的算法加大研发投入，并整合形成更强的加密原理，不能让区块链技术的安全基石完全掌握在欧美发达国家手中。

另一方面，应当增加对光纤等网络基础设施的投入，构建一个强健的主干信息网络，提升网络带宽，以应对区块链技术等分布式方式可能带来的网络容量需求的提升。

参考文献：

[1]Walport M.Distributed Ledger Technology: beyond block chain[EB/OL]. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.

[2]曹磊.区块链，金融的另一种可能[J].首席财务官,2015(24).

[3]丁未.基于区块链技术的仪器数据管理创新系统[J].中国仪器仪表, 2015(10).

[4]李大伟.比特币技术浅析[J].甘肃科技,2014, 30(24):34-35.

[5]武文斌.银行交易区块链的原理、模式与建议[J]. 河北大学学报(哲学社会科学版),2015(6).

[6]杨晓晨,张明.比特币：运行原理, 典型特征与前景展望[J].金融评论,2014(1):39-53.

[7]赵赫,李晓风,占礼葵等.基于区块链技术的采样机器人数据保护方法[J].华中科技大学学报(自然科学版), 2015(S1).

（下转第66页）

Research on the Relationship between Corporate Governance and Risk Taking of Listed Commercial Banks

Abstract: After the financial crisis, the risk management and control of commercial banks once again become the focus of attention. This article focuses on the risk taking issue of listed commercial banks in China from the perspective of corporate governance. We select the panel data of China Corporate Governance Index (CCGINK) published by China Academy of Corporate Governance of Nankai University and relevant financial data from 2009 to 2014 of 16 listed commercial banks in China for empirical analysis at three levels: corporate governance index, corporate governance sub index of all dimensions, and specific governance mechanisms. The results show that higher governance index is associated to lower risk taking; higher sub index of board governance and higher sub index of managers governance are associated to lower risk taking; the proportion of independent directors in the board of directors and shareholding of managers are negatively related to risk taking of China's listed commercial banks. Finally, this article gives suggestions for China's listed commercial banks on strengthening their corporate governance.

Key words: Listed commercial banks; Corporate governance; Governance index; Governance mechanism; Risk taking

责任编辑:金妍冰

(上接第20页)

Research on the "Impossible Trinity" of Block Chain technology and the problems should pay attention to

Abstract: Block Chain isa collection of technologies in fact.It contains three meanings: data structures, decentralized-network and security. But current technology can't meetrequirements of "efficient and low energy", "decentralized" and "security" at the same time, it exists "Impossible Trinity". In addition, the block chain technology essentially is "exchange center" rather than "eliminate center"; the whole network computing power did not generate real value; the footstone of safety is in the hands of Europe and the United State; it can't handle pressure scene and not easy for regulatory. It recommends that the Government should play an important role in the developmentof block chain technology. It needsbalance of "Impossible Trinity" in practical.The experts should try to use the computing power to resolve the meaningful questions. And we shouldmake more researcheson cryptography and other basic sciences, which related to block chain.

Key words: Block chain; BitCoin;Decentralized;Distributed Billing System

责任编辑:林庆堂