关于区块链技术应用创新与其局限性的思考

插图：张超

「摘要」近年来，区块链技术受到国内外产业、学术领域的高度重视。论文以区块链技术的原理和创新应用为研究出发点，以信用建立和安全为视角，对区块链在商业银行等领域中的创新和局限同时进行分析，最后对商业银行和其它领域的区块链技术的发展和应用提出对策和建议。

DOI:10.16127/j.cnki.issn1003-1812.2016.12.003

文 / 药晓东　冯科

近几年，区块链(block chain) 技术的研发和应用引起了学术界和产业界的高度重视，许多人认为区块链技术是未来互联网技术的一次革命，是信息基础技术的巨大创新。区块链技术的主要特点是去中心化，是基于密码学算法建立的一个全球信用的基础协议。概括来说，区块链是基于互联网的分布式账本技术，由于账本由多方共享，保证了账本的不可篡改性。

巴克莱银行于2015年9月宣布，将开始帮助慈善机构接受比特币付款，巴克莱银行也就此成为英国第一家接受数字货币的银行，也成为数字货币这一区块链技术的应用典范。在2015年12月30日，美国纳斯达克Linq系统通过其基于区块链的平台完成了首个证券交易，标志着区块链技术在主流金融系统中的成功应用。2016年1月20日，中国人民银行举行了数字货币研讨会，要求探索发行数字货币并争取早日推出央行发行的数字货币，这一数字货币背后也是区块链技术。可见区块链受到国内金融机构的高度关注并拥有广阔的应用前景。除此以外，国内外多家互联网公司，金融机构，科技企业都投入了大量的研究力量开发区块

链平台。但是由于区块链基于密码技术和通信技术，所以对于解密攻击，高效验证，压力通信和存储，以及具体应用领域的监管和效率问题格外需要注意。并且由于密码学研究的核心性与国际不均衡性，所以在区块链技术的应用上需持谨慎态度，例如银行业和其它金融领域，防止恶意攻击造成的严重损失尤为重要。

区块链的优势和应用创新

区块链技术是一种去中心化的，基于数学算法生成信任的数据库技术，其本质是一种互联网通信协议。其拥有的应用优势可以概括为：去中心化的结构相比中心化的结构可节省大量的中介成本，时间戳特征方便信息的追踪和证实问题，数学的信任机制可解决现今通信和交易的核心缺陷问题，可编程性方便在无监管的情况下履行约定。

（一）区块链技术的技术原理和特点

区块链是一种数据结构，是由最小单位区块构成，由各个区块按照时间顺序依次链接在一起，最小单位区块是交易信息的载体。为了实现可追溯性和安全性，每个区块都设计有时间戳作为标记，而且只包含两部分：1.区块头(链接到前面的区块)；2.区块体(记录了事件更新的数据)。每个区块都是依靠区块头链接到前一区块，从而形成链式结构。就通信结构来看，区块链是一个点到点的平面网格，整个网络没有严重中心化的存储和通信设备。网络中的每个节点地位对等，可同时作为用户和服务器参与数据更新和验证，并且保存所参与的全部数据信息。信任机制是通过非对称加密算法来建立的，非对称加密算法是相对于传统的对称算法而言，其特点是同时需要两个密钥：一个公钥和一个私钥。公钥和私钥是组合使用的一对，可以互相解密。例如用公钥对数据加密，那么只有用对应的私钥才能解密；用私钥加密，那么只有用对应的公钥才能解密。区块链的每个节点都拥有自己的公钥和私钥，其中公钥使全网的节点都使用相同的加密和解密算法，而私钥只有节点自己掌握。节点用自己的私钥加密，全网用户用公钥解密并验证数据来源的真实性。

区块链的技术原理使区块链技术具有三个主要特点：去中心化、可追溯性、脚本化。去中心化是指整个区块链网络中没有一个强制性的通信存储中心作为中介，取而代之的是平面的网络结构，每个节点地位对等，具有同样的通信、验证和存储的机会，任意节点可参与每一次更新和存储，所以任意节点都是整个网络的映像拷贝，少数节点的异常根本不会影响整个数据系统的运行，通过其它节点的数据足以确保系统的安全和稳健。脚本化是指区块链可以设定某一合约的写入代码，系统按照代码判断合约的执行条件并履行义务，在没有强有力的第三方监督下有效保障了合约的执行。可追溯性是指区块链上的时间戳不可被篡改，一旦生成记录，就不可撤销和退订，均锚定了交易者信息，为交易的监管带来了便利。

（二）区块链在商业银行和其他领域的研究进展及应用创新

2015年以来，区块链应用研究越来越活跃。首先解决了“拜占庭将军问题”，“拜占庭将军问题”原指战场上多个将军在彼此互不信任的情况下的一种沟通协调机制，区块链则通过数字算法设计，解决了信用的建立问题，从而实现信任和交易活动。需要强调的是，传统的信任建立是一个漫长的过程，例如商业银行的信任度的建立，是需要经过长期的时间检验和非常强的信任背书，而数字算法生成信用，直接避免了时间过程，是一种创新。

在商业银行方面，多家商业银行成立了自己的实验室，比如瑞士银行、花旗银行、纽约梅隆银行等已先后建设研发实验室，主要针对数字货币、支付和结算模式等方面尝试区块链的应用，甚至还应用于测试其员工内部系统。巴克莱银行于2015年9月宣布，开始接受比特币作为捐助货币用于慈善事业，巴克莱银行也因此成为英国第一家接受数字货币的银行。有报道称花旗银行已经创造了自己的数字货币—“Citicoin”。花旗银行透露，其内部结合了三个不同的区块链分布式总账系统，以探索更有效的方式进行价值转移。

在商业银行和区块链联盟方面，2016年4月，由42家国际银行组成的区块链联盟—R3CEV正式宣布与微软合作，致力于研究区块链底层技术和应用推广。与此之前，早在2016年1月20日，R3CEV就发布了首个分布式账本实验，并连接了巴克莱银行、BMO银行金融集团、瑞士信贷银行、澳大利亚联邦银行、汇丰

银行、法国外贸银行、苏格兰皇家银行、道明银行、瑞士联合银行、意大利联合信贷银行以及富国银行等11家成员银行共同验证实验，主要内容是这些银行在没有第三方参与的情况下，通过分布式账本上的代币资产来模拟交易。这一实验的底层框架是使用了以太坊和微软Azure的区块链服务BaaS。

在官方数字货币方面，各国政府已经频频发力，成为货币革命的决定性力量，政策推进速度更是远超预期。英国央行在2016年3月即宣布发布数字货币RSCoin代码并进行测试。2016年4月，四大会计师事务所的德勤宣布完成区块链与爱尔兰银行系统的融合，将利用区块链的优势协助爱尔兰银行完成国际投行为客户推荐投资产品项目。

根据中国最大的比特币交易平台火币网联合清华大学五道口金融学院互联网金融实验室、新浪科技发布的《2014–2016全球比特币发展报告》显示，截止到2016年6月，区块链行业获得的投资总额已经超过十亿美元。

除了银行领域，区块链技术还应用于其它金融领域、贸易交易、互联网服务、投票等领域。

在线零售方面，2015年12月，美国证券交易委员会(SEC)批准了在线零售商Overstock.com通过区块链技术发行股票的计划。Overstock.com已经开发出了一种可用于发行金融证券的区块链技术，并在此前已经用于发行私募债券，并得到实际检验，这次是同样的技术用于发行公开证券。在Overstock.com提交给美国证券交易委员会的文件中，表示该公司计划通过区块链技术最多发行5亿美元的股票和其他证券。

在保险方面，阳光保险作为国内第一家开展区块链技术的金融企业，已经于2016年3月8日推出了“阳光贝”积分应用。在“阳光贝”积分应用中，用户在享受积分功能的基础上，还可以通过“发红包”的形式将积分向朋友转赠，实现积分的流动和交易。还可以与其他公司发行的区块链积分进行互换，最大程度地活跃积分资源。

在贸易交易方面，2016年9月巴克莱银行和以色列一家初创公司共同完成了全球首个基于区块链技术的贸易交易。通过区块链技术，在4小时内完成了传统需要耗时7至10日的交易处理流程。该笔贸易结算在巴克莱银行下属的Wave公司开发的区块链平台执行完成，担保了价值约10万美元由爱尔兰Ornua公司向Seychelles Trading Company发货的奶酪和黄油产品。

（三）多国（地区）政府和央行政策推出超预期

比比特币幸运的是，多个国家和地区积极推进区块链技术的开发。为了抢占先机，重新夺回国际金融中心的地位，英国政府对金融科技企业大力扶持，给予优惠政策，积极推动金融创新，尤其是对区块链初创企业格外看重，并向全球招募区块链技术人才。为此英国央行组建了区块链技术团队，并考虑发行电子货币，以待重振昔日雄风。2016年1月3日，区块链投资公司Coinsilium在伦敦ISDX交易所IPO，成为世界上第一家成功上市的区块链技术公司。欧洲证券及市场管理局(ESMA) 2015年12月在巴黎举办的金融创新研讨会上表示，将密切关注区块链技术的发展，为监管框架调整做好准备，并将区块链和分布式账本作为专题议题进行了讨论。美国商品期货交易委员会（CFTC）表示，在技术咨询文员会会议期间讨论区块链技术及其在衍生品市场的应用，并计划把数字货币作为商品进行监管。2015年12月，美国证券交易委员会批准Overstock公司通过区块链发行自己公司的股票和其它证券。

中国央行也以十分积极的态度推进：2014年成立了团队专门研究数字货币，并于2015年进一步对数字货币的技术、流动、发行框架等各方面主题进行研究。2016年1月20日，人民银行在数字货币研讨会上以明确的态度表示支持，并争取早日推出数字货币。

（四）区块链的前景

从理论和需求的角度讲，围绕区块链这套思想和现有的开源体系能够创造非常丰富的服务和产品。区块链技术将不仅仅应用在前面所述的领域，而是将会扩展到目前所有应用范围。因为区块链将可以让人类无地域限制的、以信任的方式来进行大规模协作。纽约社会研究新学院哲学和经济理论家Melanie Swan在《区块链－新经济的蓝图》中指出，如果说区块链1.0指货币，即应用中与现金有关的加密数字货币，如货币、转账、汇款和数字支付系统等。那么区块链2.0指合约，如股票、债券、期货、贷款、智能资产和智能合约等更广泛的非货币应用；未来还可能会进化到3.0

阶段，即在政府、健康、科学、文化和艺术方面有所应用。其中区块链1.0是目前区块链技术和实践的第一步，也是最重要的一步，主要完全体现了信任的建立、通讯效率、去中心化的过程，对于区块链1.0的研究，各个领域之中，以商业银行的需求为最旺盛，但同时也是最严格。这是因为信任的建立和风险控制是区块链在商业银行业务中有效利用的根本保障，是生命所在。一旦突破区块链1.0的阶段，区块链2.0和区块链3.0都只需要结合具体目标的需要来实现。

区块链在商业银行领域进一步发展需要关注的问题和当前局限

区块链这个概念是多种技术的集合，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；三是如何确保这个网络安全运行。这三点是为了满足应用的区块链的基本思想。为了实现这三点，在技术上主要做到以下三点：可以表达先后顺序的数据结构，利用基于密码学的分布式协议构建民主网络，利用“共识机制”来确保去中心化网络的安全运行，这就是区块链技术的基本思想。尽管这样的思想在目前的应用和研究中取得一定的成绩，但是仍然存在一定的局限。

（一）密码学是安全性的基石也是最重要风险来源

密码学的安全性通常定义为所加密的信息在相当长的一段时间内无法被解密，但是随着新的数学算法的出现以及量子计算机技术的进一步发展，加密信息可能在较短的时间内被解密，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。

就目前的商业银行业务而言，如果采用区块链技术建立区块链平台，在平台上进行货币、转账、汇款和数字支付等业务，那就一定可以满足去中心化、透明化、可追溯和脚本化。但是目前的非对称加密，还不能保证在计算能力提高的情况下不被解密，因为一旦被解密，会给银行系统带来毁灭性的灾难，同时商业银行在我国的地位特殊，其重要性不言而喻。这就是为什么在研究上有不同的方法被用于航天等领域的

插图：张超

加密，例如目前在研究的量子纠缠的加密方法。如果商业银行想建立区块链平台，可以考虑更强的加密方法和技术。

在另一方面，我国密码学的发展水平还低于国际水平，相关研究主要以科技论文为主，缺乏顶尖和重大突破的研究成果，大量在实际中应用的密码产品都来自欧美等发达国家。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。

此外，以比特币为例，根据比特币的核心源代码分析，截至2015年5月14日，其中50%的源代码由三位程序员编写，而总量的近70%也仅仅只有七位程序员完成。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，这对于商业银行的应用也是一种警示，这种源代码编写人员和相关代码信息，也是一种潜在的安全风险。从商业银行的属性来看，受到攻击的潜在风险更要高于其他领域。

（二）区块链技术处理大规模信息更新和存储时其抗压能力存疑

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，在

插图：张超

交易区块链中，目前每次比特币交易大约需要10分钟，对于通过网络实现的小额电子商务交易来说，这样的处理速度显然会失去很多客户。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。从2014年到2015年，区块链的容量从14GB增长到25GB，这样大的容量需要交易用户有很高的网络带宽，使其广泛应用受到很大的影响。如果就商业银行业务而言，大量的业务和交易会使“广播风波”发生的可能性大大增加，一旦出现交易高峰，网络资源的占用就会凸显，很有可能导致业务办理的拖延。

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。

一旦有人想发起对商业银行的恶意攻击，就可以提交大量高频的信息更新要求，使整个网络的信息传递效率、验证能力和抗压能力遭受考验，即使整个网络不出现宕机，也会导致网络效率被拖慢，资源被浪费和其他信息更新的延迟，或者降低信息验证更新所参与的节点数，损失有效验证的节点数量和安全性。另外其它非法活动，也可以通过增加噪声交易的数量来增加数据的长度和存储量，使得数据读取和挖掘的耗时大大增加，以扰乱监管机构的视听。

由于可追溯性和不可撤销的信息记录，使得存储中的冗余越来越严重，即使不是恶意的污染交易，也会由于一些意外的原因造成噪声交易，特别是频繁的交易中，这种冗余会越来越严重，而真正需要监管的数据只是很小一部分。

（三）区块链技术缺乏统一的标准和生态

由于区块链技术的刚刚兴起和各机构的独立研发，使得目前区块链体系缺乏统一的技术标准，甚至像超级账本这样的大项目也依然没有统一的标准，更遑论在研发中的近千种数字货币，其技术方案更是千差万别。在存储、通讯、传输、网络安全等方面，也都未形成成熟的方案，很多实验也只是利用小规模的数据各自进行测试，也没有统一的情景和原型作为检验标准。因此说区块链的研发，缺乏协同的机制，是一个分裂的比较脆弱的生态系统。

虽然国际上有很多银行投入力量到区块链的研发中，但是对于技术力量比较薄弱、科研投入比较小的商业银行，盲目投入力量设计方案，进行区块链平台建设，很容易造成脱离实际目标、不稳定、与其他平台和应用不兼容，而导致最终失败。“群雄争霸”的根本原因就是市场和实践中未选出较优的方案“一统江湖”，这中间必然要经历不断地筛选和淘汰。

（四）商业银行自身的安全问题与区块链技术

就商业银行现状而言，有如下几个问题，需要结合区块链技术重新思考。目前的商业银行所用的系统复杂，不同的操作系统、网络协议、应用系统、不同厂家不同型号的通信设备，存储设备，计算设备，这些复杂性造成的安全性和可靠性问题，已经引起高度重视，但是这种现象是伴随着黑客技术和安全技术，以及硬件制造技术不断提高之后相伴发生的，是一种必然。商业银行开展区块链技术的应用，能否解决好代际之间的兼容性和可靠性，成为一个决定因素。此外商业银行的网络是开放性和拓展性的网络，导致网络边界模糊，同样区块链技术应用后，也无法避免这一现象，这就有可能导致关键业务系统资源被其它业务系统中的网络用户或非法人员所窥探和应用，导致出错。另一个问题就是目前的网络服务设计是基于TCP/IP协议，存在安全问题，所以区块链解决了这样

的缺陷的信任机制，但是就通信而言仍然存在地址欺骗、他人假扮身份攻击的可能性。最后由于银行不可能成为真正的去中心化的结构，所以银行的去中心化设计和多中心化或扁平化是需要进一步探讨的，所以区块链技术的应用急需就不同的业务进行仔细审视。

（五）区块链技术发展中遇到的负面声音

2016年10月31日，高盛发言人称高盛在R3的成员身份中止，紧接着西班牙桑坦德银行也宣布退出R3联盟。英国金融时报认为，高盛退出R3反映了大型银行对是否要押注区块链技术的焦虑情绪。与此同时，国际上较早研究区块链技术的企业以太坊(Ethereum)在其实验中也遇到了技术障碍，表明该项技术尚待验证。财经周刊频道2016年2月13日发布了一篇对中国人民银行行长周小川的专访，就区块链技术是否应用于数字货币，周小川指出：数字货币的技术路线可分为基于账户和不基于账户两种，也可分层并用而设法共存。区块链技术是一项可选的技术，其特点是分布式簿记、不基于账户，而且无法篡改。如果数字货币重点强调保护个人隐私，可以选用区块链技术，人民银行部署了重要力量研究探讨区块链应用技术，但是到目前为止区块链技术在使用中占用资源还是太多，不管是计算资源还是存储资源，应对不了现实的交易规模，未来还有待观察。

区块链技术应用中对商业银行和其他机构的建议

（一）商业银行在使用区块链技术时应正确对待"安全性"

由于现在区块链技术的安全性风险不能完全杜绝，所以商业银行等金融机构，需要在确保安全的基础上，提高效率和用户体验度。如果不能确保安全，那么再高的效率，再好的用户体验也是空中楼阁。所以在银行等金融领域，必须将"安全"作为首要考虑的问题，不可盲目建设和使用区块链平台，特别是核心产品和核心产品的核心技术都是由国外提供的，就更需谨慎对待。

除了数据加密，身份验证及网络安全评估之外，确保系统的可靠性和兼容性也很重要，这是由于技术更新换代引起的遗留问题。定期对重要信息再次备份，同时快速恢复被攻击的系统服务和丢失的数据，又是一个重要的问题，这个问题伴随于另一个根本问题，就是商业银行的去中心化是否可行，如果商业银行的某些业务不能去中心化，那么备份和内部信息隐藏就是必然的选择。

（二）政府应当在区块链技术的生态系统中发挥作用

政府应当在了解区块链潜在用途，建立区块链研发生态系统，建立监督管理机制等方面投入更多的力量和支持。区块链不光是技术革命，也是监管的革命，政府需要深入了解，并通过立法加强对技术代码规则的确立和监管，从而为区块链研发生态确立正确的道路，为监管寻找到高效的切入点。无论是建设全球范围的区块链系统，还是全国范围的区块链系统，确立一套高效的持续的生态系统和标准，都是关键的一步。

（三）需要加强密码学和计算能力的研究

促进核心关键技术的研发以及急需产品的开发，是任何创新领域的重中之重。对密码技术和网络安全技术的算法加大投入，以提高信任生成的保障力度，这对于各节点的安全和整个区块链平台的安全都是首要的。对数据库查询和数据挖掘算法加大投入研发，对网络基础设施和存储材料加大投入研发，是维护区块链平台稳健性和监管有效性的必由之路。特别需要强调的是，为了避免由于技术力量不对称造成的潜在国际隐患，必须在密码学这一基础学科加大研发投入。

主要参考文献：

1.ALI R,BARRDEAR J,CLEWS R, et al.The economics of digital currencies. Social Science Electronic Publishing,2014(54): 276-286.

2.KUMARESAN R,MORAN T, et al. How to use bitcoin to play decentralized poker[C]//ACM Sigsac Conference on Computer & Communications Security.c2015: 195-206.

3.LANN G L.Distributed systems-towards a formal approach.//IFIP Congress. Toronto,c1977: 155-160.

4.程华，杨云志.区块链发展趋势与商业银行应对策略研究[J].金融监管研究，2016(6): 73-91.

作者单位：药晓东　光华天成博士后科研工作站
北京大学经济学院
冯　科　北京大学经济学院