

# 【2020.2.21】《中国金融》 | 区块链技术的发展与管理

作者 | 中国人民银行数字货币研究所区块链课题组「课题组成员：穆长春 狄刚 吕远 钱友才 卿苏德」

文章 | 《中国金融》2020年第4期

习近平总书记强调“把区块链作为核心技术自主创新重要突破口”，为我国数字经济发展和产业创新实践提出了新的要求。近几年，区块链凭借其独有的信任传递机制，逐渐成为金融科技领域的热门技术，有助于业务数据可信共享，加速参与主体多方协作，实现监管穿透管理，蕴含着加速我国数字化转型、激发数字经济发展的潜力。为落实习近平总书记的指示精神，人民银行数字货币研究所（以下简称“数研所”）强化对区块链技术的基础研究和标准研制，先后推动数字票据交易平台和人民银行贸易金融区块链平台建成落地，抢占先发优势，取得了积极进展。同时，为坚决打赢三大攻坚战，对防范区块链可能引发的资产泡沫、恶意炒作、代币融资等乱象及其衍生的金融风险进行了深入调查和研究，并提出了促进区块链产业健康有序发展的思考建议。

## 区块链的技术特点

区块链是一种新型的分布式数据库，也称为分布式账本。区块链技术利用块链式结构验证与存储数据，采用共识算法生成和更新数据，借助密码学保证数据和权属安全，并通过可编程脚本代码实现数据的协同计算。

### • 区块链技术的主要优势

**一是业务数据可信化。**与传统分布式数据库有所不同，区块链引入了“人人记账”的理念，每个参与主体都有权记账，大家各自保存最新账本和所有历史记录。这种数据高度冗余的存储方式，可提升不互信主体之间的信息透明度，实现账本数据不可篡改和全程留痕，进而促进多方信息共享和协同操作。在实际业务中，通过业务数据上链，可实现纸质单据的电子化和电子信息的可信化，降低多主体之间不信任的摩擦成本，解决传统业务方式耗费大量人力物力进行单据、票据真实性审核的问题，也便于金融机构实施风险管控。

**二是参与主体对等化。**当跨部门共建信息化系统时，最大的难题在于集中存储的数据由哪个机构或部门管理。区块链的统一分布式账本技术，天然解决了“业务主权”问题，有效实现了每一个参与主体的身份对等、权力对等、责任对等、利益对等，并在所有参与主体之间实现数据的实时同步更新，使合作更加方便快捷，合作方的积极性得以提升。

**三是监管手段多维化。**监管部门可在区块链平台上增加监管节点，及时获取监管数据，并灵活定制金融监管的统计口径、监管数据颗粒度等，实现快速分析。同时，采用智能合约等可编程脚本，增加相应的监管规则，监管重点从金融机构的合规审查和风险管控，逐步上升至对系统性风险的识别监控，实现事前、事中、事后全过程的监管体系，有效防范金融风险，维护金融稳定。

### • 区块链技术存在的主要不足

**性能方面，\*\*区块链的性能和可扩展性尚有限。**\*\*在区块链中，交易只能排队按序处理，所有交易结果和支付记录都要同步到全网节点，严重影响了系统处理性能（在生产环境中，区块链系统每秒可处理逾千笔交易；实验室理想环境中，每秒交易量可能过万笔）。随着参与节点数量的增加，数据同步、验证的开销增多，系统的性能会进一步降低，从而影响区块链的可扩展性。

**安全方面，区块链缺乏体系化安全防护。**一是区块链普遍采用国际通用的密码算法、虚拟机、智能合约等核心构件，这些构件并非完全自主可控，增加了受攻击的风险。二是区块链存在内生的安全缺陷，也就是51%攻击问题（即通过掌握51%的算力重写区块链数据。下文提及51%攻击时，都是指基于算力、权益证明类共识算法的区块链）。三是区块链仍处于早期阶段，在安全方面可能存在未知漏洞。传统系

系统出现安全问题时，可采用取消、撤回、紧急干预甚至停止服务等手段。但区块链并不支持取消、撤回等相关操作。

**存储方面，全量备份的存储机制容易遇到存储瓶颈。**区块链的每个节点需存储完整的历史交易信息，当将区块链用于零售支付系统时，节点存储量将瞬时巨量膨胀。例如，2019年“双十一”，网联处理业务峰值为每秒7.15万笔，一些简易设备无法满足节点的存储需求。

**交互方面，不同区块链系统的交互性问题难以解决。**目前，相同类型的区块链之间依托定制的通信协议，可以实现数据的相互读取、验证和操作。但是，不同类型的区块链之间，由于编程语言、数据字典、系统接口、智能合约等不一致，跨链数据难互通，容易导致业务割裂。

**运维方面，业务连续性的问题不容小觑。**多方集体维护的区块链系统也会带来巨大挑战。例如，成员加入/退出、系统升级、业务规则更新等，目前尚缺乏成熟的标准、制度和操作规范，需要多方线下沟通才能处理链上的协同治理问题。

**合规方面，区块链无法保证结算最终性。**由于存在51%攻击等问题，基于区块链的支付系统无法保证结算最终性。基于区块链构建支付系统时，需考虑是否满足《金融市场基础设施原则》（PFMI）的要求，以免产生法律风险。

**职能方面，区块链的去中心化特性与中央银行的集中管理要求存在冲突。**中央银行提供的支付服务不能离开集中式账户安排，需建立在中心化系统之上，这和区块链的去中心化特性相冲突。因此，目前不建议基于区块链改造传统支付系统。

## 区块链的适用领域



区块链以大量冗余数据的同步存储和共同计算为代价，牺牲了系统处理效能和客户的部分隐私，尚不适合传统零售支付等高并发场景；但是，在对信息可信共享要求较高、对并发量要求较低的领域，例如交易结算、贸易金融、产权转让等，区块链已经有广泛应用。数研所以区块链作为技术自主创新重要突破口，从2014年开始研究法定数字货币，积极推动区块链标准化研究，探索区块链在交易结算、贸易金融等领域的金融创新。

**一是牵头制定金融分布式账本行业标准。**数研所已牵头编制金融分布式账本安全规范等多项金融行业标准，并积极参与国际清算银行（BIS）、金融稳定理事会（FSB）等国际金融标准制定组织的相关规则制定工作，也参与了国际标准化组织（ISO）和国际电信联盟（ITU）等区块链标准研制。目前，人民银行已申请了多项区块链专利，居全球央行首位。

**二是建设人民银行贸易金融区块链平台。**该平台于2018年9月4日在深圳试点成功上线，陆续开展了供应链应收账款多级融资、对外支付税务备案表、再贴现快速通道和国际贸易账款监管四项业务。通过与香港金管局的贸易联动平台签订合作备忘录，人民银行贸易金融区块链平台开启了国际化对接，未来将联合境外同类贸金平台，共同构建生态化体系。截至2019年12月17日，参与该平台推广应用的银行达38家，业务量超过870亿元。

**三是搭建数字票据交易平台。**2017年，上海票交所和数研所共同牵头开展了建设基于区块链技术的数字票据交易平台的相关工作。该平台于2018年1月25日成功在实验性生产系统上线试运行，顺利完成基于区块链技术的数字票据签发、承兑、贴现和转贴现业务，是我国将区块链技术运用到票据业务真实生产环境的首次实践。

## 与区块链相关的风险隐患



**加密资产带来的资产泡沫和金融风险。**基于区块链的加密资产无法保证其锚定资产的稳定性，甚至缺少真实资产背书，以投机交易为主，部分庄家、投机者通过对敲等手段大肆操纵加密资产的价格，导致市场剧烈波动并形成资产泡沫。截至2019年9月底，包括比特币在内的加密资产种类达到2417种，总市值突破2192亿美元。同时，部分暗网交易网站通过加密资产进行洗钱、贿赂、偷税漏税、恐怖主义融资等

违法犯罪，潜藏风险隐患较大。

**借机炒作、代币融资、骗投跑路等金融乱象卷土重来。**2019年下半年的一段时期，不少上市公司为了蹭热点，纷纷透露“上链”的动作或意图，区块链概念股一时炙手可热，甚至出现超百只个股轮番涨停的狂热行情；随着市场趋于冷静、理性，这些股票又大幅回落，纷纷跌停，许多盲目追涨的股民被高位套牢。与此同时，代币融资（ICO）之风重起，部分机构在募集资金之后携款跑路，投资者损失惨重。

**区块链的难篡改特性对舆情管控形成重大考验。**区块链技术去中心化地将信息存储在多方服务器上，其“难以篡改”的技术特性将导致信息永续留存链上，与个人信息保护中的“删除权”“更正权”存在冲突，甚至会遇到有害信息上链的问题。

## 引导区块链产业健康有序发展



**一是要去伪存真，“币”和“链”不能混为一谈。**虽然区块链发端于比特币，但区块链并不等同于比特币。区块链是密码学、对等网络、共识机制等多种传统技术的集成创新，要客观理性对待。为坚决打赢三大攻坚战，要对打着区块链幌子进行非法集资、诈骗等违法行为保持高压态势，加快市场的优胜劣汰和激浊扬清。

**二是要务实推进，不能为了区块链而搞形象工程。**对任何先进技术的作用，要相信但不迷信。正确认识区块链技术的适用场景，不是所有的项目都需要区块链，也不是所有的数据都需要上链。现阶段，区块链技术仍不成熟，面临性能、安全、标准、合规等多方面挑战，各方应冷静思考、潜心探索，切实利用区块链化解行业痛点，深度服务实体经济。

**三是要立足长远，认识到区块链技术应用系统性、长期性和复杂性特征。**目前，区块链能否做到链上链下账实相符、安全合规是行业关注的焦点。参与各方应综合考虑市场发展、风险管控、法律合规等多个维度的要求，实现链上链下联动、技术业务结合、创新与管理并重，以充分发挥“区块链+”的数字赋能潜力。

**四是要标准先行，引导区块链产业规范有序发展。**充分借鉴互联网金融风险专项整治中的经验教训，避免“先污染后治理”，特别是要关注外部性风险可能对金融安全产生的影响。制定技术标准和业务规范，可提升我国在金融区块链领域的国际话语权和规则制定权，有利于厘清区块链的“是与非”和“真伪应用”，有利于维护市场秩序和金融稳定，促进行业健康有序发展。