区块链技术在反洗钱工作中的应用前景研究

文‖中国人民银行反洗钱局课题组

作为核心技术自主创新的重要突破口，推动区块链技术发展运用已成为我国的国家战略。区块链作为一项金融科技创新技术，具有去中心化、难以篡改、可溯源的特性，可以解决金融业诸多行业痛点。近年来，随着国家总体安全观的提出，反洗钱和反恐怖融资工作作为保障金融安全和社会稳定的重要举措，越来越受到党中央和国务院的高度重视，建立和完善反洗钱、反恐怖融资和反逃税监管体制机制成为国家综合治理的重要组成部分。如何发挥区块链技术优势，将区块链技术应用于反洗钱工作领域成为极富价值和现实意义的课题。

区块链的概念和发展

区块链是按照时间顺序将数据区块以顺序相连方式组合成的链式数据结构，并以密码学方式保证不可篡改和不可伪造的分布式账本。其核心要素主要包括区块、点对点网络和共识机制三个方面。“区块”是区块链技术的主要构成要素，是区块链网络上承载数据信息的数据包，记录着包括区块创建过程中生成且经过验证的所有交易或其他数据信息；点对点网络是区块链的组网方式，每个节点都具有平等、自治的特性，具备路由发现、广播交易、广播区块、发现新节点的功能；共识机制确保各个节点可以高效地对区块数据的有效性达成共识。

相较于其他技术，区块链具有去中心化、难以篡改、可溯源等特点。在区块链网络中的每个节点均可平等参与到数据的上传、更新、接收、验证中，任何节点上传的数据都向全网广播，从而确保所有节点上存储数据的一致性和全面性；信任机制方面，由哈希算法等密码学原理保证，无需额外建立信任中介，整个系统中的每个节点之间都能进行数据交换，节点之间也不能相互欺骗，大大降低信用成本；数据以区块的形式永久储存，区块按时间顺序逐个先后生成并连接成链，使得创建期间发生的所有交易信息都能准确记录在相应的区块上，信息被分布式存储在每一个节点上，确保了数据的安全性和可追溯性。

区块链技术并不是一种单一的信息技术，而是依托于现有技术，加以独创性的整合及创新，创造一种全新的信任方式。区块链技术大致经历了三个发展阶段，即技术起源阶段、数字货币阶段和智能合约阶段。目前，区块链的应用已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。从现有应用情况来看，区块链技术具备的特性和优势，解决了一些当前金融业发展和产品革新所面临的问题和困难。可以预见，随着技术的改进以及与其他金融科技的结合，区块链技术必将逐步适应包括反洗钱领域在内的大规模金融场景的应用。

区块链技术应用于反洗钱的必要性与运用价值分析

洗钱犯罪严重影响一个国家的政治稳定、社会安定、经济金融安全，1989年金融行动特别工作组（FATF）成立以来，世界各国不断加强对洗钱犯罪行为的打击。中国在参照FATF建议以及相关国际公约的基础上，也逐步建立了适应本国国情的反洗钱体制机制，包括建立国务院反洗钱工作部际联席会议制度，确立反洗钱行政主管部门并明确主管部门和行业监管部门的职责，赋予金融机构在监测和打击洗钱犯罪中第一道防线的义务等。

从近年来的《中国反洗钱报告》可以看出，在监管部门不断强化监管的压力下，金融机构在识别客户身份、报告大额和可疑交易、保存客户身份资料和交易记录三大基础工作中的投入逐年增长。从执法检查、风险评估等监管结果看，合规性问题大幅度降低，但有效性问题逐步显现，成为阻碍反洗钱履职成效提升的瓶颈。2019年，FATF在其公布的《中国反洗钱和反恐怖融资互评估报告》中也提出“金融机构没有有效地应用尽职调查措施，在客户识别和验证措施方面存在明显的缺陷，包括受益所有人调查，以及正在进行的客户尽职调查等方面”；“没有公开可获取的关于受益所有权信息的渠道。监管当局主要利用现有的基本信息、金融机构收集的客户尽职调查信息和执法权来获取受益所有权信息”；“缺乏获得准确、充分和及时的受益所有权信息的有效制度”；“金融机构履行可疑交易报告义务的做法不一致，增加了信息泄露风险”等问题。

出于客户隐私保护、市场竞争等原

因，目前监管部门与反洗钱义务机构之间及各义务机构相互间尚未形成客户信息共享机制，多个义务机构对同一客户均需开展身份识别，投入成本高，验证渠道单一，而且识别结果往往不统一。不法分子利用义务机构数据孤岛的漏洞，进行跨机构、跨区域的资金转移，增加了义务机构可疑交易监测的难度。为发挥义务机构遏制洗钱犯罪第一道防线作用，2017 年，中国人民银行下发《关于加强开户管理及可疑交易报告后续控制措施的通知》，要求银行等义务机构在合理确认可疑交易的基础上，对可疑交易报告所涉客户、账户、资金和金融业务及时采取适当的后续控制措施。在实践中，由于缺乏必要的信息共享，对在多个义务机构开立账户进行跨机构、跨市场犯罪的涉案主体，义务机构往往未能及时采取控制措施，导致洗钱上游犯罪和洗钱犯罪活动屡屡发生。建立反洗钱共享机制，可以提升客户尽职调查工作的成本效益比，实现对确认可疑客户和可疑账户的整体管控，提升反洗钱系统的整体防御能力。

若使用传统的数据库技术实现信息共享，通常由一个中心化的运营机构来构建数据中心，数据中心负责名单的日常维护。随着接入机构数量的增加，一方面数据中心的运行压力逐步加大，影响共享数据的运行效率；另一方面数据中心面临的外部攻击风险也随之增大。一旦安全漏洞被突破，将影响所有参与共享的机构，损失难以估计，需要耗费大量资源更新和维护数据库，需要采取更高的安全措施保护数据，大大增加中心化模式下数据中心的运营成本。

与传统的数据库技术相比，区块链技术的集体维护、难以篡改与可溯源的特性，能够为反洗钱工作有效性的提高提供更多的可能。基于区块链技术的数据共享，能打通参与机构间的信息孤岛，形成完整的数据链，在兼顾隐私保护、信息安全和保密的前提下实现数据互通，释放数据价值，在此基础上，可同时赋能金融监管，并助力多方监管机制建立，形成良性治理。一方面，区块链运用分布式架构，与多方隐私安全计算平台相结合，可形成分布式安全计算，在大量数据计算需求的条件下，可以满足快速的数据信息计算和共享服务。另一方面，各个参与方的权利平等，共享数据从采集、交易、流通，以及计算分析的每一步记录都可以留存在区块链上，使得数据质量得到保证，数据安全得到强化。此外，各参与节点自主维护设备，降低了系统建设和维护成本，避免了中心化运营的弊端，具有较长的生命周期和较强的运维优势；采取碰撞匹配的信息查询方式可以进一步降低客户信息泄露的风险。

区块链技术在反洗钱工作的应用实践思路

将区块链技术运用到反洗钱领域，要伴随着法律法规的不断健全、金融基础设施的不断完备、技术领域的不断创新和应用层面的不断拓展来实现。在实践上，可采用鼓励创新、典型先试、由点及面的发展思路，并加强规范引导、促进共建共享、解决行业痛点、降低信用成本。

1. 推动义务机构建立专有链

在金融机构内部，按照区块链联盟制定的标准进行金融交易基础设施改造，以形成基于区块链技术的“私有链”。在私有链网络上，金融机构的每一个用户为一个独立节点。当金融机构采集、认证及更新用户信息时，相关信息应通过区块链技术存储和同步在每一个用户节点的本地账本中，以实现单个金融机构内部私有链网络的每个节点记录全部客户身份信息及交易信息，而区块链技术保证了信息采集更新的全流程公开透明且难以篡改。

以单一金融机构特别是大型金融机构为例，随着其产品不断创新以及各类业务操作系统的开发上线，其客户在使用新产品、新业务时可能会产生新的身份信息，但是由于各个系统的侧重点不同，对信息质量的要求也不同。目前，金融机构客户身份信息主要来源于其核心系统采集的数据，尽管在其他业务系统中也存在同一客户的身份信息数据，但这些数据并未被用于客户身份识别环节，或不能相互校验以确保身份识别的准确性，这种现象随着金融机构的扩张而愈发明显。将机构内部各个业务条线、系统作为节点建立区块链平台，将业务开展过程中获得的客户关联信息，按照社会关系、地址、联系方式、工作单位、偏好、资产规模等标签化的方式进行分类共享，金融机构内部各部门在遵循一定安全控制原则的情况下使用客户关联信息，可以突破机构内部的信息共享瓶颈，提高客户身份识别的准确度与效率。

上述做法还可进一步扩大至大型金融控股集团，将金融控股集团母公司与各子公司作为大节点搭建独立的区块链平台，多方参与，多节点维护，通过区块链存储标准结构化交易数据信息，实现金融控股集团内部数据共享，保障数据不可篡改，解决因子公司之间系统架构独立、技术指标各不相同所造成的数据标准不统一、信息不对称问题，推动子公司之间信息穿透，打通信息孤岛，从而提高整个集团客户信息一致性及可疑交易报告的准确性。

2. 建立多机构参与的联盟链

在监管机构及各金融机构间构建区块链联盟。联盟的成员包括人民银行、银

保监会、证监会等金融监管机构及银行、保险、证券、特定非金融行业等各类义务机构。联盟链网络由监管机构和金融机构两个独立的区块链大节点和其内部的私有链网络共同组成。相比于公有链，联盟链在高可用、高性能、可编程以及隐私保护上更有优势，金融机构采集认证的客户信息及交易信息在内部私有区块链认证通过后，通过联盟区块链广播、存储到所有机构节点的本地账本中，从而实现相关金融数据信息的互联共享。监管机构的参与则是引入认证控制和符合监管要求的安全标准，提高系统整体的安全可信程度。同时，可通过跨链技术实现专有链到联盟链的区块链账本间数据同步，使专有链的数据融入到联盟链的共识网络中。

联盟链的形成将在客户身份信息和交易信息两个层面实现信息共享。客户身份信息交互旨在帮助各金融机构减少客户身份初次识别和持续识别环节投入成本，解决信息不一致问题；客户交易信息共享则侧重于解决各金融机构仅可获取本机构客户交易资金流水，无法获得客户上下游资金流向的问题。

在客户身份信息共享层面，各金融机构将专有链上标准化的客户信息通过接口传输至联盟链，通过数据访问的控制逻辑实现访问者访问权限的控制。当同一客户在多家金融机构留存身份信息时，多家金融机构之间可在征得客户同意的前提下共享身份信息，而其他未与客户发生业务关系的金融机构无权访问信息的设计思路，则兼顾了防范信息泄露的风险。同时，可以考虑引入行政执法部门及司法部门的权威数据信息作为校验则可有效解决机构间互信的问题，并形成对金融机构上链数据质量的正向引导。在客户交易信息层面，随着参与节点的增多，数据同步的效率必然会受到影响，可考虑在数据预处理、增加查询处理引擎等方面进行优化。

3. 全国推广，建立全部义务机构参与的联盟链

多机构联盟链的构建需要以确保客户信息安全及保护客户隐私信息为基础。因此，在反洗钱领域联盟链构建的初期，应小范围先行试点，随着区块链技术的进步、系统建设经验的积累不断完善、逐步推开，将联盟范围扩大，最终实现建立全部义务机构参与的联盟链。

按照应用领域和性质特点划分，区块链又可以分为公共链、商业链、生活链等多种类型。因此，在建设好反洗钱领域的联盟链的基础上，还要密切关注其他能够对反洗钱工作起到辅助作用的区块链技术应用场景的拓展丰富，随着国家“双信”体系的建设，未来我们可以看到，类似于“税链”、“司法链”等一些能够有效支撑反洗钱工作的应用场景将不断出现，反洗钱义务机构的界定也将更加宽泛，适时的引入其他场景的交叉校核，更有助提高反洗钱监测分析质量。

因此，可由国家牵头开展公共区块链建设。以数字 ID 建设为起点，按照分级分类差别化管理的原则，为政府、企业、个人等不同市场主体定义数字 ID，以及与数字 ID 关联的职业信息、证照数据、资产数据、交易数据、生物特征、健康数据、网络痕迹等信息数据的分布式计算、存储、传播的算法和规则。在数据使用方面，明确密钥规则，经过法律法规和政府职能部门授权，义务机构可以核验私有数据信息。监管部门与金融机构对联盟链上的数据加以分析后生成处理结果，并将处理结果通过接口传输至所有义务机构参与的联盟链平台。链上的行政执法部门及司法部门根据收到的信息进行进一步分析处理，并将最终结果反馈至相关机构，各义务机构可据此对客户进行强化尽职调查、账户控制、销户等操作。

前景与展望

由于区块链技术特有的去中心化特性，存储数据不可篡改，同时具有开放性及可靠性，对于区块链的深入研究以及现有应用场景的分析，为解决反洗钱义务机构在现有工作中产生的问题提供了新的解决思路。分布式的存储形式也更安全可靠，确保了单一节点故障时整个网络不受影响。智能合约的应用，则可以约束联盟链之间的行为，自动监测并甄别可疑线索，主动报告洗钱行为，提升信息化水平，降低反洗钱成本。

区块链异于传统的技术特点，必然产生数据权限、隐私保护等法律层面的问题，同时也会产生技术层面的相关问题。如：数据源真实性、准确性、可信度，数据获取和使用的法律范围，客户信息隐私保护，以及参与节点的控制措施权限等等，解决好这些问题将对区块链技术在反洗钱工作中的应用起到正向作用。当前，区块链已经上升到国家战略，体现了党和国家对区块链技术发展规律的科学判断和准确把握，我国区块链技术在包括反洗钱在内的各个领域的应用势必愈加广阔和深入。尽管区块链技术本身不足以全方位地应对整个反洗钱工作所面临的挑战，但是区块链技术对于反洗钱工作有着独特的优势，能够发挥传统手段难以企及的作用。而围绕区块链技术，构建全新的机制以及配套相关政策与流程，将极大地缓解当前反洗钱工作的痛点。

（课题组成员：中国人民银行反洗钱局刘宏华、查宏、杨大立；南京分行董倩、范海鸿、贾昌峰；银川中心支行王璐）