

# 研究报告

2021 年第 31 期

2021.06.04

执笔人：陈垣桥

邮箱：

chenyuanqiao.nkhg@icbc.com.cn

## 银行业反洗钱数字化生态体系构建 及智能化转型

### 摘要：

- 本文提出“银行业反洗钱数字化生态体系”构建思路，并探讨该体系的智能化转型升级路径，以我国银行业主要数据技术痛点为切入点，提出反洗钱体系智能化转型的战略思路，构建基于人工智能技术的反洗钱数据技术痛点解决方案。

### 关键词：

- 银行业 反洗钱 数字化 生态体系 数据 智能化

重要声明：本报告中的原始数据来源于官方统计机构和市场研究机构已公开的资料，但不保证所载信息的准确性和完整性。本报告不代表研究人员所在机构的观点和意见，不构成对阅读者的任何投资建议。本报告（含标识和宣传语）的版权为中国工商银行现代金融研究院所有，仅供内部参阅，未经作者书面许可，任何机构和个人不得以任何形式翻版、复制、刊登、上网、引用或向其他人分发。

反洗钱是预防和打击金融犯罪、维护金融环境健康有序发展的重要手段。我国国务院于 2017 年印发了《关于完善反洗钱、反恐怖融资、反逃税监管体制机制的意见》，将反洗钱提升至国家战略高度。本文立足于我国银行业实际和数字化时代背景，提出“银行业反洗钱数字化生态体系”构建思路，从数字化、生态化发展角度绘制银行业反洗钱发展战略蓝图，旨在为我国反洗钱战略布局和工作开展提供参考。银行业反洗钱数字化生态体系以数字化信息的最重要载体——数据作为核心要素，数据在若干系统模块之间不断地流通和转化，形成多个整体性或局部性的“反洗钱数字化生态循环”，从而使得反洗钱体系维持稳定的动态平衡状态，并且具备自我调节、自我进化的能力。

为了提升银行业反洗钱数字化生态体系的运行效率，本文进一步提出该体系的智能化升级思路。从理论层面提出数据处理环节智能化升级的思想，并以我国银行业中的数据技术痛点为切入点，通过运用机器学习、知识图谱、智能机器人等智能技术，构建智能化解决方案。

## 一、银行业反洗钱数字化生态体系构建

本文承接研究报告《商业银行反洗钱数字化生态体系构建》，进一步探讨银行与政府部门之间、不同银行之间的相互作用和影响，从国家视角进行战略研究，构建“银行业反洗钱数字化生态体系”。



## （一）银行业反洗钱数字化生态体系框架

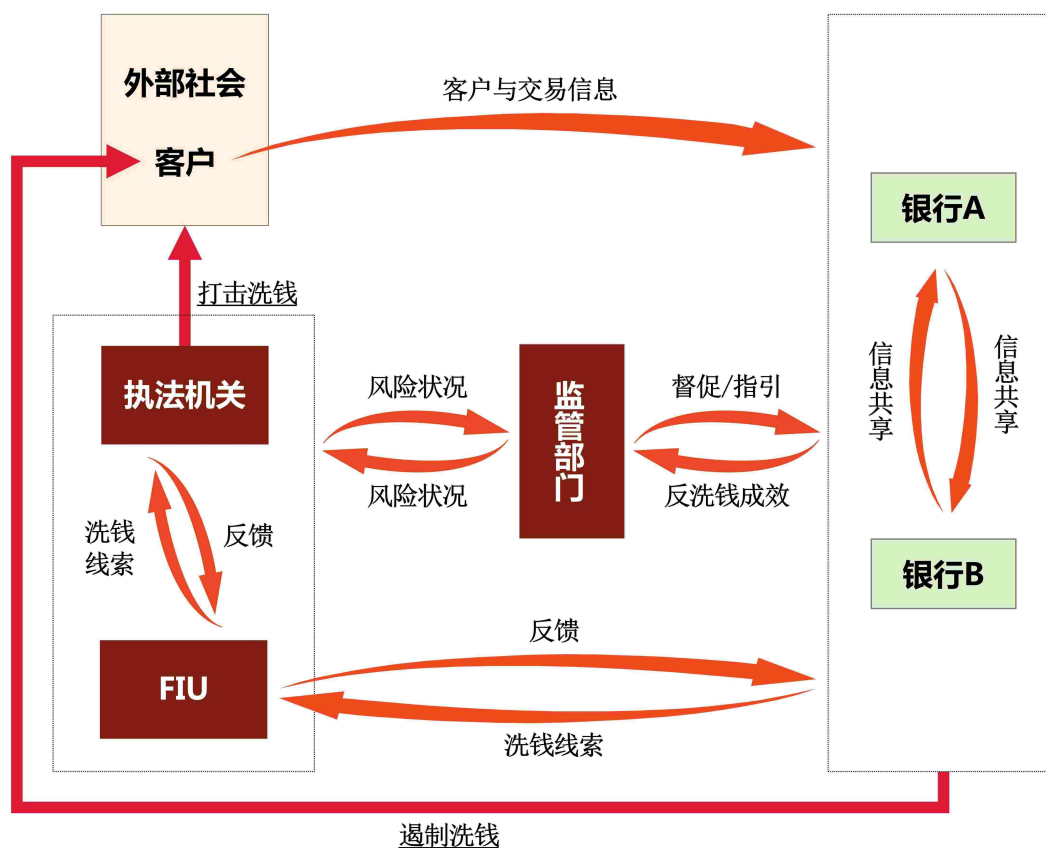


图 1 银行业反洗钱数字化生态体系框架

注：图中弯曲箭头代表数据流动，直线或折线箭头代表行动措施，箭头旁的文字概括了箭头所代表数据流动或行动措施的主要作用。

## （二）银行业反洗钱数字化生态循环

上图所示的“银行业反洗钱数字化生态体系”中，除了研究报告《商业银行反洗钱数字化生态体系构建》已经讨论过的“客户→银行→客户”、“客户→银行→FIU→执法机关→客户”以及“银行→FIU→银行”这三条数字化生态循环路径之外，还存在着另外四种数字化生态循环。

## 1. 银行间数据共享形成的循环

根据研究报告《商业银行反洗钱数字化生态体系构建》的分析，银行内部存在若干个局部性的反洗钱数字化生态循环，其中包含客户属性、客户风险、交易记录、交易风险、预防成效、控制成效等方面数据信息的流动与转化。这些数据的流转促使银行内部六大系统<sup>1</sup>的稳定运行、发展演化，那么，是否能够从这些数据中提取出一部分可与其他银行共享的数据，进而构建银行间的反洗钱数字化生态循环。这里需要解决两大关键问题：哪些数据可以共享、如何实现数据共享。本文提出以下针对这两个关键问题的解决思路。

表 1 银行间数据共享关键问题及解决思路

关键问题	解决思路
哪些数据可以共享	<ul style="list-style-type: none"> <li>➤ 客户属性、风险数据，主要包括客户身份证件、营业执照、经营范围及场所、联系方式、户籍地址、常住地址、办公地址、客户/产品/机构洗钱风险评估结果、涉及业务/产品等信息；</li> <li>➤ 交易记录、风险数据，主要包括客户通过各类渠道进行交易的时间、金额、用途以及对手方、账户余额、交易过程中的联网设备 IP 地址、设备 ID 等数据。交易数据属于金融机构特有数据，这部分数据是在金融体系内生成并存储的数据；</li> <li>➤ 银行反洗钱数字化生态体系评估结果数据，主要包括客户、产品、地域、机构、系统等维度上的评估结果。</li> </ul>
如何实现数据共享	<ul style="list-style-type: none"> <li>➤ 运用区块链、联邦学习等前沿技术，在保障数据安全的前提下，构建银行业反洗钱数据共享平台。</li> <li>➤ 建立银行业反洗钱数据标准和数据规范，统一必要字段的命名规则和数据格式，消除数据兼容性问题所造成的数据流通不畅问题。</li> </ul>

<sup>1</sup> 包括客户风险信息提取（KYC/分类）系统、交易风险信息提取（交易监测）系统、信息保存系统、事前预防系统、事中控制系统、事后控制系统，这里的“系统”是管理学概念，指的是：“由相互作用、相互依赖的若干组成部分结合而成的整体”，并不局限于日常工作中常提到的信息系统。具体内容参见研究报告《商业银行反洗钱数字化生态体系构建》。



## 2. 银行与监管部门之间的循环

当前我国反洗钱监管检查工作中存在着“以点带面”现象，即以“银行所漏报洗钱活动最终成案”这一小概率事件来衡量银行的洗钱风险防控水平。在风险为本原则之下，监管部门应从银行收集更加全面的反洗钱成效数据，作为监管措施制定和执行的主要依据。在反洗钱数字化生态体系之下，监管部门应基于银行对自身反洗钱数字化生态体系的评估结果，结合国家重点风险点，以及监管部门对银行反洗钱工作薄弱环节的推断，从而对银行反洗钱工作成效进行客观评价。这里所涉及的“国家重点风险点”和“监管部门对银行反洗钱工作潜在薄弱环节（未由银行自评估发现）的推断”，并不能仅依据经验判断而得出，而需要根据银行反洗钱成效历史数据，以及执法机关和金融情报中心（FIU）所提供的社会反洗钱状况、打击洗钱活动成效、银行情报工作成效数据，通过数据建模分析，结合定性分析，以得出符合国家银行业反洗钱实际情况的风险点定位和银行潜在薄弱环节推断。

## 3. FIU 与执法部门之间的循环

金融情报中心（FIU）对银行所提供洗钱风险情报进行分析、筛选后，提取出其中价值较大的情报，进而提交至执法部门，作为反洗钱调查、执法的重要依据。执法部门根据其反洗钱行动情况，常常会发现 FIU 金融情报工作所存在不足，于是将其反馈至 FIU，促使

其提升金融情报分析、筛选能力。这一循环能够不断促进金融情报价值的提升，从而加强国家反洗钱工作有效性。此外，FIU 在收到执法部门反馈后，可能会将一部分问题和针对性建议进一步反馈至商业银行以及其他金融机构，提升 FIU 与银行之间的反洗钱数字化生态循环有效性（关于该循环的阐述见研究报告《商业银行反洗钱数字化生态体系构建》）。

#### 4. 监管部门与 FIU、执法机关之间的循环

金融情报中心（FIU）和执法机关都可以直接接触到洗钱线索，FIU 的核心职责就是洗钱线索分析和筛选，执法机关以 FIU 所筛选出的洗钱线索作为重要依据，来开展反洗钱调查、执法工作。FIU 和执法机关可以在信息保密的前提下，将一些从洗钱线索中挖掘出来的风险状况信息分享给监管部门，使得监管部门更加清晰地了解实际洗钱风险状况，从而更加有效地开展风险为本的反洗钱监管和国家洗钱风险评估工作。

监管部门能够了解到商业银行和其他义务机构所面临的洗钱风险状况，以及这些机构所采取的反洗钱措施及其成效；此外，监管部门往往承担着国家洗钱风险评估责任，可通过该项工作获得机构、行业、国家层面的洗钱风险状况信息。监管部门可将这些信息分享给 FIU 和执法机关，为 FIU 的反洗钱情报分析和执法机关的调查、执法工作提供参考，促进打击洗钱成效的提升。





### （三）银行业反洗钱数字化生态体系评估

为了确保银行业反洗钱数字化生态体系能够切实有效地打击洗钱及其上游犯罪活动，国家政府需要定期对该体系进行评估，并对其中问题实施整改措施。银行业反洗钱数字化生态体系评估其实就是从数字化生态体系角度开展国家洗钱风险评估，也就是说，政府在建立银行业反洗钱数字化生态体系的同时，需要对国家洗钱风险评估工作进行数字化、生态化转型升级。

目前，国家洗钱风险评估主要通过风险评分卡模型进行，该类模型选取一系列用于衡量风险因素的指标，通过对这些指标加权求和得到一个风险等级，作为主要评估依据。其中权重值计算主要依赖于主观的专家经验，其合理性和有效性存在不足，且很难在较为细致的层面上针对不同情形计算差异化的指标权重，导致风险评估精细程度不足。

在反洗钱数字化生态体系视角下，国家政府应综合运用执法机关、金融情报中心（FIU）、银行、监管部门所提供的反洗钱相关数据，以及由专项调研所获取的数据，建立“数据驱动型”洗钱风险评估机制。政府可以通过引入知识图谱技术，将各家银行的洗钱风险评估结果进行关联、整合，并利用神经网络、贝叶斯网络等先进算法，对整个银行业以及整个国家的洗钱风险状况进行评估。

基于银行业反洗钱数字化生态体系评估结果，国家政府应按照风

险为本原则，对反洗钱体系中的薄弱环节进行强化，对高风险领域进行重点布局，不断提升国家反洗钱工作有效性。

## 二、银行业反洗钱体系智能化升级路径

数据作为数字化信息的最重要载体，在本文所提出的“银行业反洗钱数字化生态体系”中发挥着极其关键的作用，它就如同自然生态系统中的能量一般，驱动着整个体系的运作和发展。因此，数据运转效率直接关系到整个体系的运行效率和发展进程。人工智能技术的出现为数据运转效率提升提供了强大动力，故而如今的信息技术发展背景决定了，数字化必将走向智能化。

理论上，“银行业反洗钱数字化生态体系”中任何涉及数据处理——包括数据收集、数据信息提取、数据转化的环节都可以实现智能化升级。然而，从现实角度考虑，反洗钱体系智能化转型必然是一个漫长而艰巨的长期工程。按照风险为本原则，银行和国家政府应以当前最主要的反洗钱数据技术痛点作为切入点，通过应用人工智能技术来解决这些痛点，逐步推进反洗钱体系智能化转型升级。

### （一）我国银行业反洗钱数据技术痛点

从我国银行业视角来看，当前最主要的反洗钱数据技术痛点体现在以下四个方面。

#### 1. 洗钱风险评估

洗钱风险评估工作主要基于风险评分卡模型，其本质上是线性





多因子模型，其中参数计算主要依赖于基础性统计方法和专家经验，其数据信息挖掘能力十分有限，导致评估结果合理性和有效性不足。随着我国产业结构和银行业务结构愈加复杂化，当前洗钱风险评估模型的局限性会愈发凸显。

## 2. 可疑交易监测

银行和其他金融机构主要利用规则式模型进行可疑交易监测。规则式模型是由一组判别指标组成，只有在风险与特征变量之间完全正/负相关时才能起到较好效果，却难以从更加符合实际情况的复杂反洗钱场景中准确发掘可疑线索。根据全球范围内的统计数据，规则模型对可疑交易的命中率通常在4%左右，很难达到10%以上。这说明，规则模型产生了大量无效预警，这对反洗钱控制有效性和可疑交易报告质量产生了很大的负面影响。

## 3. 可疑交易分析

银行和金融情报中心的可疑交易甄别分析工作都严重依赖人力。随着洗钱犯罪手法不断改进、新型洗钱犯罪方式不断出现，可疑交易甄别分析工作的难度不断提升。然而，实际工作中巨大的任务量使得甄别人员难以对大部分可疑交易进行深入分析，这造成了大量的误甄别现象，对金融情报质量和反洗钱有效性造成不利影响。

## 4. 监管检查

反洗钱监管检查工作缺乏有效的数据信息收集手段和分析工

具，故而监管部门只能采用“以案倒查”这种以点带面的方式，难以形成客观、准确的监管处罚依据，间接造成了银行大量报送防御性可疑交易报告等问题。

## （二）基于智能技术的解决思路

针对上述四个方面的反洗钱数据技术痛点，本文提出以下基于人工智能技术的解决思路。

表 2 基于智能技术的反洗钱数据技术痛点解决思路

问题方面	基于 AI 技术的问题解决思路
洗钱风险评估	<ul style="list-style-type: none"> <li>➤ 运用机器学习领域前沿的 LightGBM、Xgboost 等智能算法，基于历史数据，通过特征提取、特征工程、模型训练等过程，构建高精度的客户洗钱风险智能评估模型。</li> <li>➤ 运用知识图谱，将客户、机构、行业、国家等层面的洗钱风险表征和因素相关联，进而利用神经网络、贝叶斯网络等算法对图谱网络中节点之间关系进行量化分析，实现机构、行业、国家层面的洗钱风险评估和预警。</li> </ul>
可疑交易监测	<ul style="list-style-type: none"> <li>➤ 运用机器学习领域前沿的 LightGBM、Xgboost 等智能算法，基于历史数据，通过特征提取、特征工程、模型训练等过程，构建高精度的可疑交易智能监测模型。</li> </ul>
可疑交易分析	<ul style="list-style-type: none"> <li>➤ 运用知识图谱、社会网络分析等智能技术，构建智能化辅助分析模型，对一部分规律性较强的可疑特征进行智能化提取和分析，实现交易分布特征智能提取、资金流可视化、团伙智能识别等功能，使得甄别人员能够更加高效、准确地识别和整合可疑线索，并将更多时间和精力投入到需深入推理分析的重点可疑交易。</li> <li>➤ 运用机器人流程自动化（RPA）、自然语言处理（NLP）等智能技术，构建可疑交易分析与报告辅助机器人，实现部分工作流程的自动完成，使得反洗钱分析人员能够专注于重点可疑交易分析任务，落实风险为本原则。</li> </ul>
监管检查	<ul style="list-style-type: none"> <li>➤ 运用机器人流程自动化（RPA）、自然语言处理（NLP）等智能技术，实现现场与非现场监管检查工作中的数据信息智能化采集和预处理。</li> <li>➤ 运用机器学习领域前沿的 LightGBM、Xgboost 等智能算法，基于执法机关、FIU、银行及其他反洗钱义务机构所提供数据，以及专项调研数据，建立针对“国家重点风险点”和“监管部门对银行反洗钱工作潜在薄弱环节”的智能数据挖掘模型。</li> </ul>