# 金融科技赋能下的供应链金融风险管控——基于"承兴系"诈骗案的深度思考

2015年至2019年，以罗静实控的承兴系公司为核心的供应链金融诈骗案，通过虚构与京东、苏宁等核心企业的供应链贸易，伪造应收账款300余亿元，最终造成80余亿元损失，成为金融科技时代供应链金融风险管控的典型反面教材。该案暴露了传统风控体系在数字化背景下的脆弱性，也揭示了金融科技在风险识别、预警与处置中的关键作用。本文以"承兴系"事件为切入点，结合金融科技发展现状，探讨供应链金融风险管控的创新路径。

1. 事件复盘：传统风控体系的失效与漏洞

承兴系诈骗案的核心在于利用传统风控体系的三大漏洞实施系统性欺诈。其一，虚假贸易背景的隐蔽性。罗静团队通过伪造与核心企业的采购合同，将虚构应收账款包装为底层资产，利用核心企业信用背书骗取金融机构融资。传统风控过度依赖核心企业信用，忽视对贸易真实性的穿透核查，且各环节风控独立运作，缺乏全链条数据整合能力。其二，伪造公章与合同的技术性。案件中，罗静团队通过伪造公章、虚构合同、控制对公账户等手段，构建了完整的虚假贸易链条。传统风控依赖人工审核纸质文件，难以识别数字化伪造技术，暴露了流程管控的滞后性。其三，核心企业信用捆绑的累积风险。承兴系将多家核心企业的应收账款打包融资，形成"信用捆绑"效应。一旦单一核心企业风险暴露，将引发系统性连锁反应，凸显传统风控对核心企业过度依赖的脆弱性。

二、金融科技赋能：风险管控的范式革新

金融科技为供应链金融风险管控提供了技术重构的可能性。首先，大数据与人工智能构建智能风控模型。通过区块链技术实现贸易合同、物流单据、资金流水的实时上链，确保数据不可篡改；利用机器学习对供应商交易行为建模，识别异常交易模式，如频繁更换供应商、账期异常拉长等。其次，区块链技术重塑信任机制。将贸易合同条款转化为智能合约代码，实现融资发放、还款、质押物处置的自动化，减少人为操作风险；通过分布式账本共享核心企业、金融机构、物流方的贸易数据，解决信息孤岛问题。最后，物联网与数字孪生实现动态质押物监管。在质押物仓库部署传感器，实时采集温度、湿度、位置等数据，防止质押物被替换或转移；构建质押物三维模型，与物联网数据联动，实现远程可视化监管。

三、实践案例：金融科技风控的落地应用

金融科技风控已在部分机构实现落地应用。某国有银行通过构建汽车供应链金融风控体系，整合核心企业ERP系统、物流企业WMS系统、金融机构信贷系统数据，建立企业信用画像；根据供应商交易频次、回款周期、质量合格率等指标，实时调整授信额度；引入信用保险，当供应商违约时，由保险公司承担80%损失。某股份制银行在电子科技供应链金融中，针对电子元器件价格波动风险，为企业提供期货套保方案设计，锁定原材料成本；与大宗商品交易所合作，建立质押物价格实时监测系统，当价格下跌超过10%时自动触发补仓或处置机制。

四、挑战与对策：金融科技风控的持续优化

金融科技风控的推广仍面临技术、监管与协同三大挑战。技术层面，数据孤岛问题导致核心企业ERP系统、金融机构信贷系统数据格式不统一，需建立标准化接口；算法黑箱风险使AI风控模型可能忽视新型诈骗模式。监管层面，隐私保护与数据共享的矛盾需在区块链共享贸易数据时符合《个人信息保护法》《数据安全法》要求；智能合约法律效力需立法明确司法认定标准。针对上述挑战，建议建立行业级风控平台，由中物联、银行协会牵头构建供应链金融数据共享联盟；加强监管科技（RegTech）应用，监管机构利用自然语言处理技术实时监测金融机构供应链金融业务舆情；完善应急处置机制，建立供应链金融风险准备金制度，当发生重大风险事件时由行业协会统筹处置。

五、结论：金融科技重构供应链金融生态

"承兴系"诈骗案揭示了传统风控体系在数字化时代的失效本质。金融科技通过大数据、区块链、物联网等技术，实现了从"人工经验驱动"到"数据智能驱动"的范式转变。未来供应链金融风险管控需以技术为底座，构建全链条数字化风控体系；以协同为核心，推动核心企业、金融机构、物流方、监管机构数据共享；以合规为边界，在技术创新与监管要求间寻找平衡点。唯有如此，才能实现供应链金融"风险可控、成本可降、效率可升"的发展目标，真正服务实体经济。