智能合约驱动的跨领域数据全生命周期自动化流通管控机制研究

高丽，杨昊，倪雄
上海市大数据中心，上海 200072

DOI: 10.61369/TACS.2026090012

摘　　要： 跨领域数据流通是数字政府、航运贸易、金融风控与供应链协同的核心基础，但现有流通模式普遍存在主体信任缺失、授权边界模糊、审批繁琐、状态异步、异常处置滞后等突出问题。传统人工审批与中心化共享模式，难以适配多主体、高频次、高合规约束的跨领域数据协同场景。本文融合联盟链、智能合约等技术，提出一种智能合约驱动的数据全生命周期自动化流通管控机制。该机制以联盟链为可信底座、智能合约规则引擎为核心，将数据登记、申请、审批、授权、使用、交割、熔断、归档等流程建模为事件驱动的可验证状态机，通过代码化落地分级管控、最小必要、场景匹配等合规规则，实现数据流通从“事前审批”到“事中控制”的连续管控。本文结合航运贸易、政务审批、金融风控、供应链协同典型场景验证机制可行性，并梳理智能合约安全、预言机可信、跨链协同等核心挑战。研究证明，智能合约可将静态制度转化为可执行、可溯源、可同步的跨主体协同能力，为跨领域数据可信合规流通提供标准化管控框架。

关 键 词： 自动化审批；数据授权；交割存证；异常熔断

Research on the Automated Lifecycle Management Mechanism of Cross-Domain Data Flow Control Driven by Smart Contracts

Gao Li, Yang Hao, Ni Xiong
Shanghai Municipal Big Data Center, Shanghai 200072

Abstract: Cross-domain data circulation is the core foundation for digital government, shipping trade, financial risk control, and supply chain collaboration. However, the existing circulation models generally have problems such as lack of trust among entities, ambiguous authorization boundaries, cumbersome approval processes, asynchronous status, and lagging abnormal handling. The traditional manual approval and centralized sharing models are difficult to adapt to cross-domain data collaboration scenarios involving multiple entities, high frequency, and strict compliance requirements. This paper integrates technologies such as consortium chains and smart contracts to propose an intelligent contract-driven automated circulation control mechanism for the entire data lifecycle. This mechanism uses the consortium chain as the trusted base and the smart contract rule engine as the core, modeling the data registration, application, approval, authorization, use, delivery, melting, archiving, etc. processes as event-driven verifiable state machines. Through the code implementation of hierarchical control, minimum necessity, and scenario matching compliance rules, it realizes continuous control of data circulation from "pre-event approval" to "in-process control". This paper validates the feasibility of the mechanism in typical scenarios such as shipping trade, government approval, financial risk control, and supply chain collaboration, and discusses core challenges such as smart contract security, oracle trustworthiness, and cross-chain collaboration. The research proves that smart contracts can transform static systems into executable, traceable, and synchronized cross-entity collaborative capabilities, providing a standardized control framework for cross-domain data trustworthy and compliant circulation.

Keywords: automated approval; data authorization; delivery and evidence storage; abnormal melting

引言

数字经济时代，数据要素跨领域流通已从简单接口共享升级为多主体全流程协同，航贸、政务、金融、供应链领域对可信数据流通的需求持续提升。当前跨领域数据存在资源分散、规则繁杂、信任缺失等问题，造成共享效率低、合规风险高、权责界定不清。现有研

项目基金：2024年度国家“区块链”重点专项课题“航运贸易跨部门数据接入及流通管理关键技术研究，课题编号：2024YFB2705403。

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

究多聚焦区块链架构、访问控制与宏观治理制度，缺乏面向数据全流程的自动化管控体系。本文聚焦智能合约的流程管控核心价值，构建数据流通全生命周期状态机与模块化规则引擎，搭建标准化自动化流通管控机制，适配多类跨领域业务场景。本文核心贡献为：搭建跨领域数据流通标准化状态模型，设计可配置智能合约规则引擎，多场景验证机制落地价值并明确治理边界。

一、相关研究综述

（一）区块链、智能合约与可信状态管理

区块链凭借分布式防篡改、多方共识特性，成为多主体数据协同的可信基础设施，适用于共享状态记录与关键行为存证，无需承载原始业务数据。相关研究证实，智能合约可实现跨组织业务流程自动化管控与信任构建，有效破解跨主体协同信任壁垒。当前行业已经形成主流技术共识：采用链上存储目录标识、授权状态、数据哈希与操作摘要，链下留存原始数据与业务系统，兼顾流通可信性与数据隐私，为本文流通状态机建模提供坚实理论支撑[1]。

（二）业务流程自动化与合约化执行

BPMN2.0是业务流程标准化建模的通用规范，可实现跨领域数据流通流程的规范化拆解与落地。现有研究聚焦 BPMN 模型与智能合约的融合路径，重点解决链上流程执行、链下事件触发、外部数据接入等核心难题。针对区块链依赖链下数据的短板，业界依托预言机实现链上智能合约与链下业务数据的联动交互。同时形成清晰的分层设计思路：业务人员定义流通场景与规则，平台转化为标准化智能合约逻辑，技术人员负责智能合约运维与安全审计，有效规避智能合约代码黑箱问题。

（三）访问控制与数据治理标准

ABAC 属性访问模型与零信任架构，构建了细粒度、动态化的数据授权范式，摒弃固定网络信任逻辑，实现每次数据调用的独立合规校验。ISO27001、NIST 隐私框架及欧盟数据治理法规，明确跨领域数据流通需满足合规管控、隐私保护、风险可控的核心要求。现有理论与标准充分证明，传统单次鉴权模式已无法适配跨领域流通需求，亟需构建覆盖全流程的持续性合规管控体系[2]。

（四）预言机和智能合约安全治理

智能合约只可以识别链上状态，依靠预言机实现链下业务数据接入，预言机的可信度直接决定智能合约执行精度。为了规避单点预言机的风险，行业内一般使用多源校验、签名认证、时间戳溯源等方式来加以改良。由于智能合约存在代码漏洞、规则固化、升级困难等安全问题，所以用模块化开发、上线审计、版本控制、应急熔断等手段来保证运行安全。

二、跨领域数据流通的问题分析

（一）传统审批模式不能适应高频协同的需求

当前跨领域数据流通依靠人工审批、线下核验和中心化调度，航贸单证核验、政务跨部门审批、金融授信等场景中存在审批链路过长、材料重复提交、流程状态不透明等问题。多方合作的时候会遇到审批成本高、风控压力大、监管溯源难的问题，很多高价值的数据因为流通效率不高而无法得到利用，大大限制了数据要素的价值发挥。

（二）流通规则分散，执行标准不统一

跨领域数据流通有数据分级、主体资质、用途限定、最小必要、跨网传输等多种规则，目前规则分布在制度、合同、平台配置和人工经验里，没有统一的执行入口。在多场景下使用数据的时候，由于人工审批标准不一、记录残缺、权责不清，容易产生合规风险和业务纠纷[3]。

（三）授权与使用行为脱节，事中管控缺失

传统数据共享模式重审批、轻管控，授权发放后没有持续的行为校验，超范围、超期限、超频次、跨场景调用等违规行为只能事后审计发现。在金融、航贸等高敏感场景中，滞后的事后处置模式不能实时规避数据安全和合规风险，管控漏洞明显。

（四）数据交割缺少可信存证依据

现有的流通只保留了基础接口日志，不能覆盖数据校验、接收确认、交割闭环等核心环节，也没有统一可信的交割凭据。数据交割的时间、内容、主体不能准确溯源，在数据滥用、信息泄露、贸易纠纷时无法确定责任，严重影响跨领域协同公信力。

（五）异常处置滞后，风险防控能力薄弱

超权限调用、超频访问、数据篡改等异常行为只能通过事后巡检、审计来发现，不能做到事前预防和事中阻断。由于缺乏自动化的风险识别和熔断机制，造成数据流动过程中的风控处于被动地位，不满足跨领域流通所要达到的高安全性、高合规性的要求。

三、智能合约驱动的全生命周期自动化流通管控机制设计

（一）总体架构

本文提出了一种三层结构的构建，即链上可信控制层、链下业务执行层、跨领域接口适配层。链上依靠联盟链、智能合约规则引擎来进行状态管控、规则执行、存证固化；链下对接各方的业务系统和网关服务，负责原始数据的存储以及安全传输；适配器使用专门的网关来实现多平台、多网域的格式转换和状态回调。涵盖数据拥有者、使用者、监管机构等重要主体的身份认证机制，支持主流的身份认证协议，聚焦“授权是否有效、范围是否匹配、状态是否可用”。

（二）生命周期状态机建模

本文把数据流通全流程标准化为登记、申请、审批、授权、

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

使用、交割、暂停、撤销、过期、归档状态。所有的状态变更按照可追溯、独立控制、全量校验、异常优先的原则来进行，变更记录完整地保留了主体、时间戳和规则版本，从而达到全流程可追溯的管理效果。

（三）模块化智能合约规则引擎

智能合约规则引擎是机制的核心，把主体资质、数据分级、使用场景、授权阈值等多个参数综合起来，得出标准化的管控决策。将引擎拆分为策略管理、流程控制、授权执行、风险熔断四个模块化的智能合约，采用“模板固定、参数可配、版本可溯”的架构，确保核心流程稳定，支持业务规则动态迭代，有效兼顾系统稳定性与业务灵活性[4]。

（四）分层自动化审批机制

数据申请提交之后，智能合约依照形式校验和实质合规校验的次序来进行审核，进而形成三级审批机制，即低敏标准化场景全自动审批，中敏风险场景实行限制性条件审批，高敏、跨境核心数据自动转入人工复核。自动化审批只代替标准化重复工作，保留人工裁量和监管入口，兼顾流通效率和风险安全。

（五）动态授权和状态管理

审批完成后，生成唯一的授权标识，并与主体、场景、字段、有效期、调用频次等重要权限要素绑定。授权状态支持实时监测、动态变更以及事件订阅，在出现授权过期、资质失效、异常访问等情况时会自动更新状态，并将最新的信息同步到网关上，保证所有请求都是符合当前规定的情况下进行处理的。

（六）全维度数据使用校验

采取链下网关快速校验、链上关键节点核验的分层方式，兼顾性能和安全。高频低风险调用使用网关缓存校验，高敏数据、首次调用、异常操作强制链上核验。从主体、状态、范围、场景、环境、行为六个方面进行全过程校验，全面杜绝各种违规访问行为。

（七）链上链下协同交割存证

机制把业务数据流和管控管理流分开，原始数据经链下加密通道传输保证隐私和效率，交割核心哈希值、授权信息、双方签名、时间戳等关键数据上链存证，形成完整的交割闭环，给业务核验、权责界定、纠纷处置提供可信依据。

（八）分级异常熔断机制

创建出五级异常熔断体系，对于各类违规和异常情形作出分级管控，根据风险等级来开展告警、限流、暂停、撤销以及监管介入等管控动作。另外还设置了白名单、灰度阈值和人工恢复机制，在对风险进行精准防控的时候不会对核心业务造成任何影响。

（九）事件驱动式状态同步

针对多链、多平台异构环境，用事件驱动架构来完成状态同步，智能合约在关键节点状态变化时自动发送事件，链下适配器实时更新网关缓存。通过全局唯一的流通 ID 和版本号机制来避免状态冲突，在链上管控状态和链下执行状态不一致的时候优先按照高安全等级的状态来进行处理，保证跨平台、跨系统的数据流通状态统一[5]。

四、跨领域应用场景

（一）航运贸易场景

聚焦航贸单证核验、电子放货、信用证再融资三个主要场景，达到多方数据自动化可信验证。对提单、舱单、港口作业、海关放行等单证的核验规则通过智能合约固定，用以代替手工重复核对；整合各个方面的放货条件，符合条件就自动更新放货状态，异常情况就会熔断。融资环节里精细限定数据使用范围以及用途，兼顾贸易真实性核验与商业隐私保护，解决航贸多主体协同效率低下、纠纷繁杂等问题。

（二）政务协同场景

适配政务跨部门审批和联合监管的需求，把法定审批规则、数据共享边界、最小必要原则固化成智能合约逻辑。可以实现多部门数据并行核验、状态实时同步，减少群众和企业材料重复提交。针对差异化监管需求，根据企业风险等级选择不同的数据调用策略，低风险主体简化核验流程，高风险主体强化管控，同时保留行政裁量入口，符合政务合规治理的要求。

（三）金融风控场景

应用于授信审批、保理融资、保险理赔等业务，解决传统人工尽调真实性低、成本高、数据滥用等问题。授信审批中，用智能合约把融资场景和数据调用权限联系起来，金融机构只能拿到风控必须的数据。保理融资中，智能合约自动核验订单、发票、物流、仓单数据的一致性，识别出重复质押、单证造假等风险。保险理赔中，异常熔断机制可以拦截高频异常申请、违规数据调用，提高金融风控精准度和效率。

（四）供应链协同场景

供应链订单协同、仓单流转、产融对接的全部过程，依靠智能合约对订单、入库、质检、质押等重要节点的数据流状态进行控制。规范仓单质押数据调用权限，防止重复质押、信息不对称现象发生；根据供应链多级主体动态变更的特点，订单拆分、主体迭代、多平台状态同步等都可以被适配，采用轻量化的适配器来适应中小企业原有的系统，并且不需要过多的改造工作，使整个供应链的数据可以被有效地管理和流通起来。

五、挑战与展望

（一）智能合约安全、迭代治理

智能合约代码漏洞会造成数据安全和业务风险，必须创建全生命周期的安全管控体系，涵盖建模、开发、审计、灰度发布、运维监控等所有过程。将智能合约拆分成多个模块，降低智能合约的复杂性，形成多主体协同的版本治理机制，实现规则动态迭代，适应行业监管和制度更新的要求。

（二）预言机可信性优化

链下数据可信接入是智能合约精准执行的前提，单点预言机存在数据篡改、失效的风险。未来要建立多源预言机校验、可信执行环境、数据签名溯源体系，依靠多个主体对数据进行交叉比对，提高链下事实的校验精度，明确数据接入的责任边界。

 Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

（三）合规与法律效力的衔接

智能合约可以做到对标准规则的自动执行，但是不能包括法律解释、行政裁量等柔性场景。之后要打通智能合约执行记录和法律制度、商业合同之间的连接渠道，确定自动化执行和人工复核的范围，赋予链上存证、智能合约执行结果的法律证据效力。

（四）性能、成本和隐私的平衡

高频数据流通场景下，全量上链存在着性能瓶颈以及隐私风险。需要对分层存证策略进行改进，高频低风险操作聚合上链、核心敏感操作实时存证，并且用通道隔离、数据加密、字段最小化的方式实现流通性能、运营成本、数据隐私安全的三者兼顾。

（五）跨链标准化建设

多行业异构链共存是长期存在的现象，亟需统一的数据目录、授权状态、交割存证、异常事件跨平台标准。依照目前各行业的建设准则来创建航贸、政务、金融和供应链等领域的专属智能合约模板和接口规范，进而增强跨区域以及跨行业复制推广力度。

六、结论

跨领域数据流通的主要痛点不是数据传输能力的缺失，而是全流程管控的标准化、自动化、可信化能力不足。文章利用联盟链、智能合约等技术创建起一个有关数据登记、申请、审批、授权、使用、交割、熔断、归档等全过程自动化的管理系统，实现规则代码化、流程状态化、风险前置化与可信存证，解决了旧式流通行程慢、管控弱、追责难以及责任模糊等弊端。该机制可以很好地适配到航运贸易、政务协同、金融风控、供应链协同这些重要的场景中去，落地性好，也具备很高的扩展能力。智能合约本质是数据治理制度的可执行载体，未来要持续开展智能合约标准化、链下可信接入、法律效力衔接研究，实现技术管控和制度治理的融合，给数据要素市场化流通提供坚实的支撑。

参考文献

[1] 欧盟委员会。欧洲数据战略 [COM(2020) 66 最终版][S/OL]。2020. 网址：https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066

[2] 欧盟委员会。关于共同欧洲数据空间的工作人员工作文件 [SWD(2022) 45 最终版][S/OL]。2022. URL: https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces

[3] Szabo N. 公共网络中关系的建模与保障 [J]. First Monday, 1997, 2(9). DOI: 10.5210/fm.v2i9.548. URL: https://firstmonday.org/ojs/index.php/fm/article/view/548

[4] Nakamoto S. 比特币：一种点对点电子现金系统 [EB/OL]。2008. 网址：https://bitcoin.org/bitcoin.pdf

[5] Yaga D, Mell P, Roby N, Scarfone K. 区块链技术概述 [R]. NISTIR 8202，美国国家标准与技术研究院，2018年。DOI: 10.6028/NIST.IR.8202。URL: https://csrc.nist.gov/pubs/ir/8202/final

Copyright © This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License