基于 DID 与可验证凭证的跨领域数据精准授权与权责配置机制研究

倪雄，杨昊，高丽
上海市大数据中心，上海 200072
DOI: 10.61369/TACS.2026090013

摘　　要： 跨领域数据流通已迈入多主体、跨网域、跨行业协同阶段。航运贸易、政务服务、金融风控和供应链协同等场景普遍存在主体信任薄弱、数据权责模糊、授权链条冗长、授权状态核验滞后、权限回收不及时等痛点。传统基于账户、角色、密钥的授权模式，无法满足跨领域数据流通精细化、可溯源、可撤销的治理需求。本文依托 W3C 分布式标识符（DID）、可验证凭证（VC）核心标准，构建面向跨领域数据流通的三方协同精准授权与权责配置机制。该机制以数据授权方、使用方、持有方为核心主体，通过 DID 搭建跨领域可验证身份体系，依托 VC 标准化承载授权范围、使用期限、业务目的、权责主体与撤销状态，结合可验证表述（VP）与状态服务实现数据调用前验证与动态权限管控。本机制将传统纸质化、弱验证的线下授权转化为机器可读、可追溯、可撤销的数字化凭证体系，可为航运贸易核心场景及政务、金融、供应链等衍生场景提供标准化、可复用的数据治理技术框架。

关 键 词： 可验证凭证；精准授权；三方授权；权责配置；授权撤销

Research on Cross-Domain Data Precise Authorization and Responsibility Allocation Mechanism Based on DID and Verifiable Credentials

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

Abstract: Cross-domain data circulation has entered a stage of multi-party, cross-domain, and cross-industry collaboration. In scenarios such as shipping trade, government services, financial risk control, and supply chain collaboration, there are common problems such as weak trust among entities, ambiguous data rights and responsibilities, lengthy authorization chains, delayed verification of authorization status, and insufficient timely recovery of permissions. The traditional authorization model based on accounts, roles, and keys cannot meet the requirements for refined, traceable, and revocable governance of cross-domain data circulation. This paper builds a three-party collaborative precise authorization and responsibility configuration mechanism for cross-domain data circulation based on the core standards of W3C Distributed Identifiers (DID) and Verifiable Credentials (VC). This mechanism takes the data authorizer, user, and holder as the core entities, builds a cross-domain verifiable identity system through DID, relies on VC to standardize the authorization scope, usage period, business purpose, responsibility subjects, and revocation status, and combines verifiable representation (VP) and state services to achieve pre-data invocation verification and dynamic permission control. This mechanism converts the traditional paper-based and weakly verified offline authorization into a machine-readable, traceable, and revocable digital voucher system, which can provide a standardized and reusable data governance technology framework for core scenarios in shipping trade and government services, finance, and supply chain and other derivative scenarios.

Keywords: verifiable credentials; precise authorization; three-party authorization; responsibility configuration; authorization revocation

引言

数据要素跨领域流通的核心瓶颈并非数据传输技术，而是跨组织、跨监管边界的可信授权与权责界定。如航运贸易场景涉及货主、港口、海关、金融机构等多元主体，汇聚贸易单证、物流信息、企业经营等敏感数据。传统线下授权、接口白名单、中心化账号模式，

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

难以支撑高频、细粒度、可撤销的跨领域数据调用需求。跨领域数据授权涉及数据授权方、使用方、持有方三类核心角色，权责关系复杂，亟需标准化技术体系厘清身份、权限、用途、责任的对应关系。DID 与 VC 技术可实现身份去中心化验证、授权关系数字化表达、权限状态动态管控，有效弥补传统授权机制短板。基于此，本文构建跨领域三方精准授权与权责配置机制，聚焦数据授权确权、动态管控、权责绑定核心问题，适配多行业数据流通场景，为数据要素合规高效流通提供技术支撑。

一、相关研究综述

（一）DID 与 VC 标准化进展

W3C DID Core v1.0标准实现了主体标识与中心化机构的解耦，可通过密码学技术完成身份控制权验证，能够为跨领域数据流通全参与主体、数据资源、服务接口提供统一的可信标识层。W3C VC Data Model v2.0进一步完善了凭证数据模型、有效期、状态管理与隐私安全规范，定义了签发者、持有者、验证者的三方核心生态。同时，OpenID4VCI/OpenID4VP 系列规范完善了凭证签发、出示与核验的标准化协议，打通了 DID/VC 技术落地业务系统的接口层，实现跨设备、跨平台的授权交互闭环，为产业化应用奠定了标准基础[1]。

（二）自主身份与数字凭证研究进展

自我主权身份（SSI）理论强调主体对身份凭证的自主管控，具备跨领域互认、最小披露、可携带的核心优势。现有研究已明确 SSI 的核心组件与技术架构，实现了从个人身份认证向组织、设备、数据资源标识的延伸。当前研究已从基础架构探索转向场景化落地，但大多聚焦个人身份核验与资格证明，针对跨行业数据流通的多方权责匹配、精细化授权场景的研究仍较为薄弱，难以适配多主体协同的数据授权治理需求。

（三）授权、访问控制与数据空间研究

传统 OAuth2.0、ABAC 访问控制模型可实现基础的接口权限与属性化动态授权。ODRL 策略模型可标准化表达数据使用许可、约束与责任，为精细化授权规则提供语义支撑。数据空间相关规范则确立了跨领域数据流通的合约协商、资源发现、安全传输体系，明确了跨组织数据共享的信任框架。现有技术体系可支撑数据流通基础架构，但缺乏将主体授权同意、用途约束、权责界定转化为可验证数字凭证的落地路径，无法实现授权全流程自动化、可溯源管控[2]。

（四）现有研究不足

综合现有研究，当前 DID/VC 相关技术与理论已趋于成熟，但面向跨领域数据精准授权的落地体系仍存在显著短板。一是多数研究聚焦个人身份认证，忽视数据授权三方主体的权责划分；二是传统访问控制技术无法生成可迁移、可撤销、可验证的跨领域授权凭证；三是数据空间体系缺乏主体授权与合规管控的标准化凭证载体；四是授权状态动态管理、实时撤销与权限回收机制不完善，存在合规风险。

二、跨领域数据授权的问题分析

（一）数据权责边界模糊

跨领域数据由多主体协同生成、加工。权属、使用与存储高度分离。数据授权方真实权益地位难以在传统授权体系中体现；数据使用方的业务场景、使用需求差异化显著；数据持有方仅掌控数据资源与接口，不具备完整授权决定权。传统“持有即授权”的逻辑与线下书面授权模式，导致权责主体错位、边界模糊，无法适配精细化治理要求[3]。

（二）授权链条缺乏机器可验证能力

当前跨领域授权多依托纸质文件、线上勾选、API 密钥等方式，仅能证明授权事实，无法被业务系统自动解析、核验。授权主体、范围、期限、用途、有效性等核心要素分散，导致授权核验效率低、人工成本高、风险识别滞后，无法形成自动化、标准化的跨领域授权验证闭环。

（三）授权粒度与业务场景不匹配

传统二元化“允许 / 拒绝”授权模式粒度粗糙，无法适配细分业务场景需求。跨领域数据流通需要基于业务目的、数据字段、使用时长、操作类型、应用场景实现差异化授权，而传统 RBAC、ABAC 模型无法同时满足细粒度权限管控与可携带授权证明的双重需求，易出现超范围数据使用问题。

（四）授权撤销与权限回收滞后

数据授权具备时效性与可撤销性，授权撤回、业务终止、主体资质变更、密钥风险等场景均需即时回收权限。但现有授权凭证多为长期有效，系统仅校验签名完整性，不实时核验授权状态，极易出现“凭证有效、授权失效”的合规风险，无法实现动态权限管控。

（五）跨领域互认与隐私保护冲突

跨领域授权互认过程中，固定身份标识与状态查询链路易导致用户行为、业务场景被关联追踪，引发隐私泄露问题。现有机制难以平衡跨领域可信核验与隐私最小披露的核心需求，制约了技术的规模化落地。

三、基于 DID/VC 的精准授权与权责配置机制设计

（一）设计目标与原则

本文机制以“身份可证、授权可验、范围可控、状态可查、责任可配、撤销可达”为核心目标，遵循五大设计原则：一是主体标识与业务身份分离，依托 DID 实现去中心化身份验证，通过 VC 承载业务资质与角色属性；二是授权凭证与访问执行分离，VC 承载授权规则，数据持有方、API 网关、连接器负责数据访问；三是构建“主体 – 数据 – 操作 – 目的 – 时间 – 责任”多维精准授权语义；四是优先校验动态授权状态，规避静态签名的时效性风险；五是兼顾隐私最小披露与权责可审计，实现安全与合规双向保障。

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

（二）角色模型与信任关系

机制构建三方核心角色体系，完全适配 W3C VC 标准生态。数据授权方为数据权益主体，负责确认授权范围、用途与期限，并完成数字签名确认；数据使用方为业务需求主体，负责发起授权申请、持有凭证、合规使用数据；数据持有方为数据管控主体，负责核验凭证、执行权限管控、保障数据安全。三方角色分别对应 VC 生态的签发者、持有者、验证者，可通过行业可信机构完成代理签发，适配多场景复杂授权需求，明确各主体权责边界[4]。

（三）DID 标识层设计

搭建统一 DID 标识体系，覆盖主体、服务、资源三类核心对象。主体 DID 适配自然人、企业、机构及系统代理身份；服务 DID 标识授权签发、状态核验、数据验证等业务接口；资源 DID 唯一标识数据集、API、数据字段等数据资源。DID 文档集成验证方法、认证关系、服务端点，结合场景适配 did:web、did:ion 等多类技术方案，兼顾跨领域互认、密钥轮换、隐私防护与监管可追溯性。

（四）授权 VC 数据模型

授权 VC 为机制核心载体，构建模块化字段体系，涵盖凭证元数据、主体绑定、数据范围、使用目的、操作权限、责任配置、状态管理、安全证明八大模块，标准化定义授权有效期、参与主体DID、可调用数据粒度、业务场景、操作约束、权责条款、授权状态与安全依据。模型融合 ABAC 属性授权与 ODRL 策略规范，支持精细化权限约束与外部策略引用，实现授权语义标准化、机器可解析[5]。

（五）三方协同授权流程

设计六阶段全流程授权闭环：一是数据使用方提交数据授权申请，明确使用场景、数据范围、期限与安全承诺；二是数据授权方核验授权申请信息，签名确认授权意愿；三是可信授权服务依据申请信息与授权签名，签发绑定唯一使用方的授权 VC；四是数据使用方通过 OID4VP 协议提交 VP 凭证，发起数据调用请求；五是数据持有方完成身份、签名、授权范围、状态的全维度核验，合规则放行数据；六是持续管控授权状态，支持冻结、撤销、过期更新，实时回收违规、失效权限。

（六）精准授权策略

构建多维动态授权判定模型，以数据使用方 DID、数据资源 DID、操作类型等为基础，叠加业务用途、授权期限、数据字段范围、指定业务场景、有效凭证状态、合规义务约束多维度条件，实现细粒度精准授权。针对航运、政务、金融、供应链等差异化场景，定制场景化授权规则，杜绝超范围、超用途、超期限数据调用。

（七）授权凭证状态管理与动态撤销

建立多状态凭证状态机，涵盖注册、签发、有效、冻结、撤销、过期、失效七大状态，适配临时管控、主动撤回、资质失效等差异化场景，实现凭证状态高效、隐私化批量核验，规避单凭证查询的关联风险。同时，明确授权撤销触发条件，授权失效后即时阻断新的数据调用，同步规范存量数据的后续使用、删除与合规处置流程。

（八）与既有技术体系的衔接

本机制不替代现有技术架构，可与 OAuth2.0、API 网关、数据空间等深度融合。通过 OAuth 获取访问令牌，将 VC 标准化授权语义转化为短期可执行访问权限，依托现有数据空间的资源发现、合约协商、传输管控能力，叠加 DID/VC 的身份可信认证与合规授权能力，形成“合约约束 + 凭证授权 + 网关管控”的多层级治理架构，兼容现有业务系统，降低落地成本。

四、跨领域应用场景

（一）航运贸易场景

作为核心应用场景，可支撑提单核验、报关单查询、信用证融资、电子放货、保险理赔等核心业务。货主、贸易企业作为数据授权方，限定银行、保险、货代等数据使用方仅可在指定融资、核验场景下调用单证、物流数据，明确字段范围与使用期限。港口、海关、船公司等数据持有方通过实时核验凭证状态，杜绝超权限使用，解决传统纸质授权真伪难辨、权限回收滞后的问题，提升航运贸易数据流通效率与安全性。

（二）政务数据共享场景

适配政务跨部门数据共享需求，企业、个人可生成事项专属授权凭证，允许审批部门仅在对应办事场景下查询纳税、社保、资质等政务数据，替代传统部门白名单模式。实现政务数据“一事一授权、限时可撤销”，支撑“免证明办事”“最多跑一次”政务改革，兼顾数据共享效率与个人企业信息权益保护。

（三）金融风控场景

应用于征信查询、授信风控、保险理赔等场景，通过 VC 标准化绑定客户授权意愿、查询范围、使用期限与合规责任。解决金融行业线下授权核验繁琐、权限边界模糊、溯源困难等问题。实现金融数据查询合规化、精细化管控，降低机构运营风险与用户信息泄露风险，适配金融行业高安全、高合规要求。

（四）供应链协同场景

针对供应链数据敏感、协同复杂的特点，实现订单、仓单、物流、库存数据的最小必要授权。核心企业、金融机构、物流企业仅可获取自身业务所需的细分数据字段，禁止二次转发与商业化使用，有效规避商业机密泄露风险，支撑供应链金融、产融协同等业务合规开展。

五、机制评价维度

本文机制可从六大核心维度验证有效性：一是授权准确性，实现全维度授权语义精准表达与超权限调用精准拦截；二是跨领域可验证性，无需统一中心账户体系即可完成跨主体可信核验；三是撤销时效性，实现授权失效后快速状态更新与权限回收；四是隐私最小化，通过场景化标识、选择性披露降低用户信息关联风险；五是业务可用性，适配现有系统架构，交互简洁、落地成本低；六是合规支撑性，全面适配数据流通知情同意、最小必

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

要、可追溯、可撤销的合规要求。

六、挑战与展望

当前机制落地仍存在若干短板：DID 与真实主体绑定缺乏完善制度支撑，跨行业授权语义尚未统一，隐私保护与实时核验存在技术张力，数字凭证法律效力有待明确，用户交互体验仍需优化。未来将构建行业授权模板与语义词表，完善工程集成方案，平衡核验效率与隐私安全，推进数字授权凭证合规落地。

七、结论

跨领域数据流通的核心痛点是可信授权缺失与权责边界模糊。本文基于 DID/VC 标准化技术体系，构建了三方协同的跨领域数据精准授权与权责配置机制。通过 DID 实现跨领域可信身份标识，通过结构化授权 VC 承载精细化授权规则与权责关系，通过 VP 核验与动态状态管理实现数据调用前验证与动态权限管控，兼容传统授权架构与数据空间体系。该机制重点适配航运贸易场景，同时可快速迁移至政务、金融、供应链等多领域，有效解决了传统授权模式权责模糊、核验滞后、权限不可控、无法溯源等问题。可为跨领域数据要素合规、高效、安全流通提供标准化技术治理方案，为后续数据授权体系的工程化落地与行业标准化建设提供理论支撑。

参考文献

[1] 万维网联盟 . 可验证凭证使用案例 [S/OL].W3C 小组备忘录，2026年 .URL: https://www.w3.org/TR/vc-use-cases/.

[2] Sporny M.，Guy A.，Sabadello M.，Reed D. 分布式标识符（DIDs）v1.0：核心架构、数据模型和表示 [S]. W3C 推荐标准，2022年 . URL: https://www.w3.org/TR/did-core/.

[3] Sporny M.，Thibodeau T.，Herman I.，Cohen G.，Jones M. B. 可验证凭证数据模型 v2.0[S]. W3C 推荐标准，2025年 . URL: https://www.w3.org/TR/vc-data-model-2.0/.

[4] Sporny M.，Longley D.，Prorock M.，Alkhraishi M. 位字符串状态列表 v1.0：用于可验证凭证的隐私保护状态信息 [S]. W3C 推荐标准，2025年 . URL: https://www.w3.org/TR/vc-bitstring-status-list/.

[5] Longley D.，Sporny M.，Herman I. 可验证凭证数据完整性 1.0：保障可验证凭证数据的完整性 [S]. W3C 推荐标准，2025年 . URL: https://www.w3.org/TR/vc-data-integrity/.

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