面向个人数据流通的三方授权条款建模与可验证自动交付机制

吴超辉[1]，高建彬[2]，宋蒴鑫[2]，马　英[3]，管庆旭[4]，夏　琦[2]，夏　虎[2]，冯　春[1]
（1. 66015部队，北京　100192；2. 电子科技大学，四川　成都　611731；
3. 国家信息中心，北京　100045；4. 四川省大数据中心，四川　成都　610043）

摘　要：针对个人数据流通中数据持有方、个人与数据使用方三方授权边界不清、交付过程难验证和争议责任难追踪等问题，提出一种三方授权条款建模与可验证自动交付机制。该机制构建由主体域、数据域、约束域和责任域组成的授权条款模型，并结合去中心化身份、数字签名与智能合约，实现条款注册、状态演化、一次性交付令牌签发和交付回执锚定；在链上规则存证与链下受控交付协同架构下，形成“授权生效-条件校验-自动交付-结果验证-审计追责”的闭环。实验结果表明，该机制能够在链上开销可控的前提下支持条款驱动的自动交付，在异常交付识别率和可追责性方面优于对比方案。

关键词：个人数据流通；三方授权；授权条款建模；智能合约；自动交付
中图分类号：TP309　　**文献标志码**：A　　DOI:10.19358/j.issn.2097-1788.2026.07.010

中文引用格式：吴超辉，高建彬，宋蒴鑫，等. 面向个人数据流通的三方授权条款建模与可验证自动交付机制[J]. 网络安全与数据治理，2026，45(7)：71-79.
英文引用格式：Wu Chaohui，Gao Jianbin，Song Shuoxin，et al. Three-party authorization clause modeling and verifiable automatic delivery mechanism for personal data circulation[J]. Cyber Security and Data Governance，2026，45(7)：71-79.

Three-party authorization clause modeling and verifiable automatic delivery mechanism for personal data circulation

Wu Chaohui[1], Gao Jianbin[2], Song Shuoxin[2], Ma Ying[3], Guan Qingxu[4], Xia Qi[2], Xia Hu[2], Feng Chun[1]
(1. Unit 66015, Beijing 100192, China; 2. University of Electronic Science and Technology of China, Chengdu 611731, China;
3. State Information Center, Beijing 100045, China; 4. Sichuan Provincial Big Data Center, Chengdu 610043, China)

Abstract: To address the problems of unclear tripartite authorization boundaries, difficulty in verifying the delivery process, and challenges in tracing dispute liability in personal data circulation, this paper proposes a tripartite authorization clause modeling and verifiable automatic delivery mechanism. The proposed mechanism constructs an authorization clause model consisting of the subject domain, data domain, constraint domain, and responsibility domain. By integrating decentralized identity, digital signatures, and smart contracts, it enables clause registration, state evolution, one-time delivery token issuance, and delivery receipt anchoring. Under a collaborative architecture combining on-chain rule notarization and off-chain controlled delivery, the mechanism establishes a complete closed loop of "authorization activation - condition verification - automatic delivery - result verification - audit and accountability". Experimental results show that the proposed mechanism can support clause-driven automatic delivery while keeping on-chain overhead controllable, and outperforms comparative schemes in terms of abnormal delivery identification rate and accountability.

Key words: personal data circulation; tripartite authorization; authorization clause modeling; smart contract; automatic delivery

0　引言

随着数据要素基础制度持续完善，个人数据逐渐由静态信息资源转变为可授权、可流通的数据要素。在医疗、金融、政务服务、社交平台和工业互联网等场景中，个人数据通常由医院、平台企业或行业机构等数据持有方保存；与此同时，科研机构、商业机构、政府部门和算法服务商等数据使用方，也不断提出在合法合规前提下的数据利用需求。因此，个人数据流通并非简单的双方共享问题，而是涉及数据持有方、个人和数据使用方的三方协同问题。

现有个人数据授权实践多依赖平台协议、静态电子同意书或中心化权限表，难以对授权主体、授权对象、使用范围、使用目的、期限、费用和违约责任等要素进行结构化表达。即使授权关系已经形成，后续数据交付过程仍可能出现超范围调用、过期使用、交付内容与约定不一致、平台留痕不完整和争议责任难认定等问题。区块链、去中心化身份（Decentralized Identity，DID）和智能合约为授权状态存证、条件校验和审计追踪提供了技术基础，但现有研究多集中于同意管理、访问控制、医疗数据共享或交易审计，尚未充分解决授权条款如何直接驱动可验证自动交付的问题。

综合现有研究，个人数据流通仍存在三方面不足：第一，角色设计多采用数据主体-控制者-处理者或患者-医院-第三方等场景化表达，缺少面向数据持有方、个人和数据使用方的一般化三方抽象；第二，授权表达多停留在字段策略或访问权限层面，尚未形成可约束使用范围、期限、费用、违约和争议处理的授权条款模型；第三，自动执行通常止步于允许访问或允许下载，对交付条件、交付结果、回执验证和事后追责缺少统一闭环。

针对上述问题，本文提出一种面向个人数据流通的三方授权条款建模与可验证自动交付机制。该机制以数据持有方、个人和数据使用方为基本主体，将授权对象、使用范围、用途、期限、费用、撤回、违约和争议处理等要素映射为可验证、可执行的授权条款；通过链上规则存证与链下受控交付协同，实现条款生效后的条件校验、一次性交付令牌签发、数据包交付和回执锚定；并利用日志存证与审计验证支撑异常识别和责任追踪。

本文的主要贡献如下：（1）构建面向个人数据流通的三方授权条款模型，统一描述主体、数据、约束和责任要素；（2）设计授权条款的智能合约表达与状态演化机制，使授权状态能够联动后续交付资格；（3）提出基于一次性交付令牌和回执摘要的可验证自动交付流程；（4）设计异常交付识别、日志留痕和争议处理机制，形成“授权生效-条件校验-自动交付-结果验证-审计追责”的闭环。

1 相关工作

1.1 动态同意与个人数据授权管理

个人数据授权管理研究首先关注如何将“同意”转化为可记录、可撤回和可执行的技术对象。在已有研究中，Merlec 等提出基于智能合约的动态同意管理系统，使数据主体能够在生命周期内授予、查看、更新和撤回同意，并通过区块链记录授权历史与日志[1]。Peyrone 等利用形式化方法描述同意授权、撤回、续期和服务请求过程，并将模型映射为智能合约原型，以增强同意管理过程的正确性[2]。Daudén-Esmel 等进一步区分数据收集同意与数据处理同意，分别设计智能合约以支持授权授予、撤回、修改和验证[3]。

在医疗和物联网等具体场景中，动态同意研究进一步强调同意状态的透明性、版本管理和可追溯性。Benchoufi 等面向临床试验场景，利用区块链对患者同意和再同意过程进行时间戳记录，使同意状态能够与试验协议版本绑定，从而增强临床试验中同意收集过程的透明性和可追溯性[4]。Rantos 等提出 ADvoCATE 平台，面向物联网个人数据处理场景，支持数据主体对同意进行生成、更新和撤回，并通过区块链和智能合约维护同意的完整性、不可否认性和版本信息[5]。Albalwy 等提出 ConsentChain 架构，面向临床基因组数据共享场景，利用智能合约支持患者授权、撤回授权、数据请求验证和链下数据访问控制，并将同意元素表示为机器可读形式，以提升动态同意和数据访问过程的自动化能力[6]。

Truong 等则指出，区块链更适合作为认证、授权和审计基础设施，真实数据交付宜由链下系统完成，以降低高频数据取回带来的复杂度和开销[7]。总体来看，上述研究证明了动态同意、授权撤回、版本管理和链上审计在个人数据授权中的必要性，但其重点仍主要停留在同意状态管理和访问授权层面，对费用、期限、违约责任、争议处理以及交付条件等条款化要素支持不足，也尚未将授权条款与后续自动交付、交付回执和责任追踪统一建模。

1.2 区块链环境下的数据共享与交易审计

在个人数据与医疗数据共享场景中，区块链常与链下存储、加密访问控制和完整性验证等机制结合，以提升数据访问的可控性和可审计性。Zyskind 等提出将区块链作为个人数据访问控制管理器，通过链上记录权限和数据指针、链下保存加密数据，使用户能够控制服务方的数据访问[8]。Azaria 等提出 MedRec 系统，利用智能合约记录患者-医疗机构关系、访问许可和数据指针，支持跨机构电子病历索引、审计和授权共享[9]。张磊等提出云链协同的电子医疗病历可控共享模型，将病历密文存储于链下云端，并将数据摘要和访问策略写入联盟链，结合属性加密与可搜索加密实现病历可控共享和完整性校验[10]。上述研究表明，

链上保存摘要、权限和审计线索，链下保管原始或密文数据，已成为个人数据和医疗数据共享中的典型设计思路。

在具体数据共享与交易审计方面，牛淑芬等提出基于区块链的电子病历共享方案，通过链上索引与链下密文存储支持授权后的安全访问[11]。李亚红等进一步引入密文正确性验证机制，说明数据共享不仅需要访问许可，还需要验证交付内容的完整性和正确性[12]。在数据交易和跨域流通场景中，张正昊等通过监管凭证和授权凭证实现敏感数据可控共享与追责[13]；张川等面向跨联盟链数据交易，关注交付真实性、支付公平性和收据可验证性[14]；郝嘉琨等基于去中心化身份构建跨域数据交易系统，强调身份可信绑定和合规联动[15]。上述研究为链上链下协同、访问权限管理、交付验证和审计追踪提供了基础，但整体仍更多面向共享、交易或医疗数据管理场景，授权关系通常停留在患者授权、访问许可或交易凭证层面，尚未将数据持有方、个人和数据使用方之间的三方授权条款与自动交付过程统一建模。本文在这些工作的基础上，进一步面向个人数据流通场景，将授权条款、状态演化、交付令牌、回执锚定和争议追责纳入同一闭环机制。

1.3 智能法律合约与本文定位

智能法律合约研究关注如何将自然语言合同条款转化为可执行、可验证和可审计的程序逻辑。孟疏桐等提出智能法律合约驱动的联邦学习数据授权和执行方法，利用形式化语言表达授权协议，并结合去中心化身份标识、数字签名、分布式文件系统（InterPlanetary File System，IPFS）和区块链存证实现身份认证、条款执行和证据保全[16]。该研究说明，将授权协议形式化并映射为智能合约规则，能够为数据协作中的身份可信、过程留痕和证据固定提供技术支撑。

但智能合约的公开透明特征也可能带来隐私泄露风险。王有恒等系统梳理了区块链智能合约隐私保护技术，指出智能合约在交易数据、参与方身份、合约状态和执行逻辑等方面均存在隐私暴露风险，并总结了可信执行环境、零知识证明、安全多方计算和同态加密等保护技术[17]。这些方案虽能增强合约隐私保护能力，但仍存在性能开销大、部署复杂、通用性不足和责任边界不清等问题，因此不宜将完整授权条款、交付内容和敏感业务过程直接上链。

基于上述研究，本文采用链上链下协同思路，链上仅保存授权条款摘要、状态标识、交付令牌、回执摘要和审计证据，链下完成原始数据存储、权限校验和受控交付。与既有研究相比，本文重点不在于提出新的底层隐私协议，而是面向个人数据流通中的三方关系，统一建模授权条款、交付条件、状态演化、交付回执和责任追踪，形成“授权生效-条件校验-自动交付-结果验证-审计追责”的闭环机制。

2 方法

针对现有研究中三方关系抽象不足、授权表达停留在策略层、自动交付缺乏可验证闭环等问题，本文在链上规则存证与链下受控交付协同架构下，提出一种由三方授权条款驱动的自动交付方法。该方法吸收了形式化同意管理、可控共享、跨域身份解析与智能法律合约等研究中的有益思想[2,13-16]，但不直接复用其场景设定，而是面向一般个人数据流通场景，对主体关系、条款字段、状态演化和交付验证进行统一建模。

2.1 设计原则与总体框架

方法设计遵循四项原则：一是主体清晰，即将数据持有方、个人和数据使用方作为最小授权单元，避免将数据控制者、处理者等概念直接照搬到具体业务场景；二是条款可执行，即授权不再仅以访问控制字段存在，而是将范围、目的、期限、费用、违约责任等转化为可校验的合约项；三是交付可验证，即把交付条件、交付结果和交付回执纳入统一流程；四是数据最小暴露，即区块链只保存条款摘要、状态和验证凭据索引，原始个人数据仍由链下持有方受控保管。

基于上述原则，框架由身份与签名层、条款建模层、链上执行层和链下交付层组成。其中，身份与签名层负责完成三方身份绑定与授权签署；条款建模层负责生成可执行条款实例；链上执行层负责条款存证、状态更新与条件校验；链下交付层负责交付令牌验证、数据包发送、回执生成和审计留痕。具体框架如图 1 所示。

2.2 三方授权条款模型

设数据持有方记为 H，个人记为 P，数据使用方记为 U。与传统二元授权不同，本文认为个人数据流通的核心不是“谁访问数据”，而是“谁基于何种身份，在何种范围内，以何种目的使用由谁持有的数据”。因此，授权条款实例被抽象为由主体域、数据域、约束域和责任域四类字段组成。

主体域用于描述 H、P、U 的去中心化身份标识、签名公钥和角色属性；数据域用于描述数据对象标识、数据类别、版本、敏感等级和最小交付单元；约束域

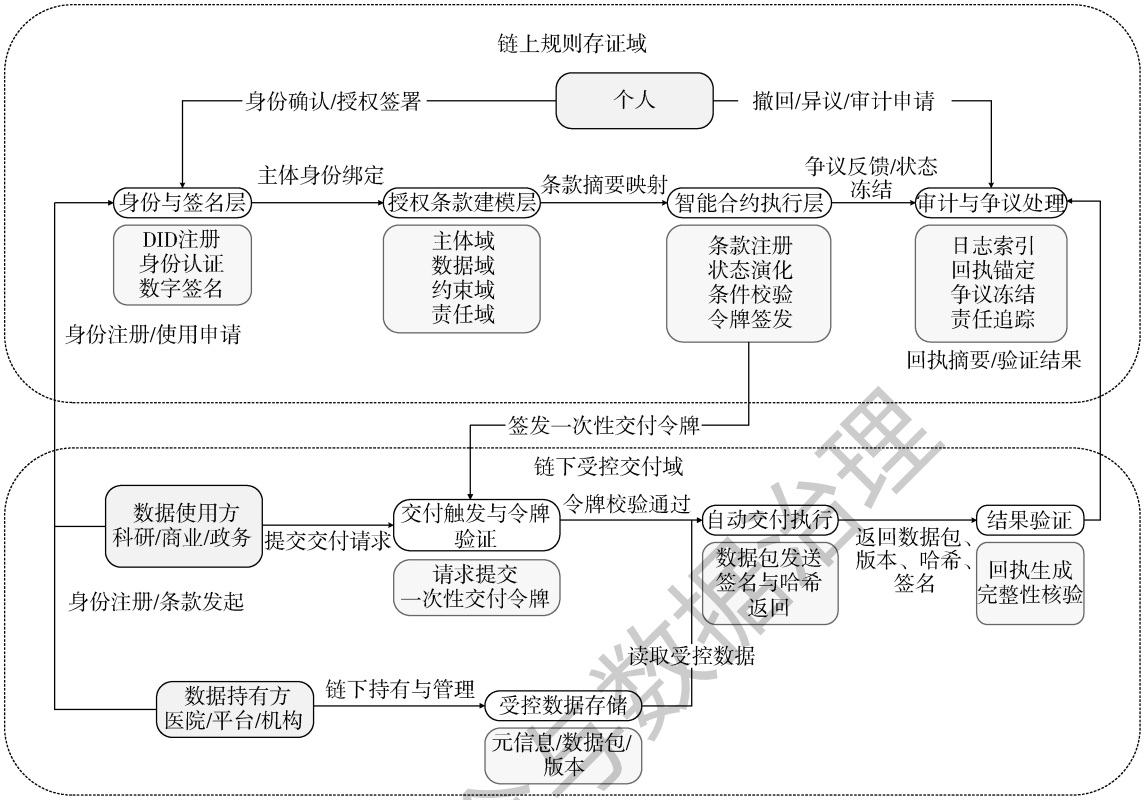

图 1　面向个人数据流通的三方授权与可验证自动交付总体框架

用于描述授权范围、使用目的、交付方式、有效期、次数上限和费用条件；责任域用于描述撤回条件、违约处理、争议机构和审计要求。由此可将一个授权条款实例记为：$T=<\mathrm{id_H}, \mathrm{id_P}, \mathrm{id_U}, \mathrm{obj}, \mathrm{scope}, \mathrm{purpose}, \mathrm{valid}, \mathrm{quota}, \mathrm{fee}, \mathrm{remedy}>$。其中，obj 表示授权对象，scope 表示授权范围，valid 表示有效期，quota 表示次数或频率限制，remedy 表示违约与争议处理规则。

参考形式化同意模型与智能法律合约模板，本文进一步将条款生命周期定义为 Draft、Offer、Confirm、Active、Suspend、Revoke、Expire、Dispute 和 Close 九类状态。状态迁移不是任意发生，而是由事件触发：当数据持有方发布条款实例后，状态由 Draft 转为 Offer；当个人和数据使用方完成身份认证与签名确认后，状态转为 Confirm；当保证金、许可费或外部合规条件满足后，状态转为 Active；当出现撤回、超期、争议或违规回执时，状态分别转入 Revoke、Expire 或 Dispute。该设计使授权变更能够直接联动后续交付资格，而非只停留在静态记录层。

2.3　面向条款执行的智能合约映射

为避免链上明文泄露和过度存储，本文采用“条款明文链下保存、条款摘要链上注册、关键状态链上演化”的映射方式。具体而言，条款文本或结构化 JavaScript 对象表示法（JavaScript Object Notation，JSON）由持有方本地保存或存入受控对象存储，其摘要值 h_T、参与主体 DID、数据对象标识、当前状态、回执索引和审计索引写入合约。链上合约提供 registerClause( )、confirmClause( )、activateClause( )、revokeClause( )、issueToken( ) 和 submitReceipt( ) 等方法，以驱动条款执行。

在身份侧，借鉴去中心化身份和证书绑定机制，H、P、U 均需完成 DID 注册，并提交与条款相关的签名证明。合约仅接受通过身份认证的主体发起状态变更。为了避免一方单独篡改条款，confirmClause( ) 要求至少包含 H 和 P 的双签，涉及收费或持续使用时还需要 U 的确认签名。该机制实质上把“要约-承诺”过程转化为链上可检验事件。

在数据侧，考虑到个人数据常由医院、平台或行业机构代为保存，链下数据对象不直接由合约托管。为此，本文将数据对象分为元信息、数据包和验证值三层：元信息包括数据对象标识、版本和用途标签；数据包为待交付内容本体；验证值包括数据包哈希、签名和可选的密文完整性证明。这样，合约只需验证条款有效性与交付条件，真正的数据发放仍由链下持有方完成。

2.4 可验证自动交付协议

在上述条款模型和合约映射基础上，本文设计可验证自动交付协议。协议由条款创建、条款激活、交付触发、交付执行和结果验证五个阶段组成。

（1）条款创建。数据持有方生成条款实例 T，个人对授权对象、用途、期限等核心字段进行确认，数据使用方对费用与使用条件进行确认；完成双签或三签后，由合约登记条款摘要并返回唯一条款地址。

（2）条款激活。合约检查条款签名、保证金、许可费、监管许可等外部条件。若条件满足，则将状态置为 Active，并写入可用次数、到期时间和可交付对象标识。

（3）交付触发。数据使用方提交请求 $\mathrm{req}=<\mathrm{addr}_T, \mathrm{id}_{\mathrm{req}}, \mathrm{ts}, \mathrm{nonce}>$。合约验证请求方身份、条款状态、剩余额度和时效性。若验证成功，则签发一次性交付令牌 token，同时记录本次请求的时间戳和请求序号。

（4）交付执行。链下交付节点验证 token 后，从持有方受控存储中提取与 obj 对应的数据包或密文片段，并向使用方发送数据包 D_{pkg}、版本 ver、数据哈希 h_{pkg} 以及持有方签名 $\mathrm{sig}_{\mathrm{H}}$。为降低交付争议，交付节点还需返回条款地址和请求序号，确保数据包与具体条款实例一一绑定。

（5）结果验证。数据使用方对收到的数据包进行完整性核验，并生成回执 $\rho=H(\mathrm{addr}_T \| \mathrm{id}_{\mathrm{req}} \| h_{\mathrm{pkg}} \| \mathrm{ver} \| \mathrm{ts})$。随后，使用方将回执摘要、验证结果和签名提交至合约。若回执验证通过，则合约扣减额度并将状态记为 Delivered；若验证失败，则转入 Dispute，并冻结后续同条款交付。

该协议相较于仅凭访问控制放行的传统方案，新增了“交付令牌”和“回执摘要”两个中间对象。前者用于把一次请求与一次交付绑定，避免“一次授权、无限下载”；后者用于把链下结果重新锚定回链上状态，便于事后审计。其思想与敏感数据共享中的凭据校验、跨链数据交易中的收据验证以及电子病历共享中的完整性检查是一致的，但本文将其统一纳入三方授权条款框架之中。

2.5 审计与争议处理机制

考虑到个人数据流通常伴随用途争议、超期使用和交付不一致等问题，本文设计链上审计与争议处理机制。其核心不是对原始数据进行二次公开，而是对授权-请求-交付-回执全过程形成最小充分证据。具体包括四类日志：条款注册日志、状态变更日志、交付触发日志和回执验证日志。四类日志均以哈希索引形式上链，必要时由持有方、使用方和审计方提交链下原文进行一致性校验。

当出现以下任一条件时，合约触发争议流程：一是交付数据哈希与条款登记版本不一致；二是交付时间晚于有效期；三是额度已经耗尽但仍重复签发令牌；四是个人已撤回授权但请求仍被执行。进入 Dispute 状态后，合约冻结同条款后续调用，并向审计节点开放最小必要证据接口。审计节点依据条款摘要、请求摘要、回执摘要及相关签名完成复核，从而实现可追责处置。该处理方式能够兼顾证据保全与隐私最小暴露，符合智能法律合约研究中“执行-违约-仲裁”的基本逻辑。

2.6 部署边界、信任假设与制度衔接分析

在实际部署中，本文机制定位于个人数据流通业务中的上层授权治理与交付控制层，而非替代现有数据库、对象存储或行业业务系统。链上部分主要承担条款摘要存证、状态演化、交付令牌签发和回执锚定等控制功能；链下部分由数据持有方或其受控交付节点保存和发送数据对象。该设计避免了原始个人数据直接上链，也将高频、大体量的数据传输从区块链执行逻辑中剥离出来，从而降低链上存储和执行开销。

本文机制建立在以下信任假设之上：联盟链共识节点不被单一主体完全控制，能够保证条款状态、令牌和回执记录不可随意篡改；数据持有方在条款注册阶段提交的数据对象标识、版本号和哈希值能够代表待交付数据对象的基准状态；链下交付节点可能出现延迟、故障或返回错误数据，因此需通过一次性交付令牌、数据哈希、持有方签名和使用方回执进行约束；审计节点仅在争议状态下基于最小必要证据进行复核，不默认获取原始个人数据明文。从制度衔接看，主体域、数据域、约束域和责任域可分别映射授权主体、数据类别、处理目的、使用范围、有效期限、撤回和争议处置等要求。本文机制不直接判断条款法律效力，而是提供可记录、可执行、可验证和可追责的技术支撑。

2.7 方法分析

本文方法将三方主体、授权条款、状态机、交付令牌和回执验证纳入统一闭环，弥补了现有工作中“授权”和“交付”相互分离的问题。通过“条款地址-请求序号-交付令牌-数据哈希-回执摘要”的绑定关系，链下交付过程能够重新映射为链上可验证事件，使系统不仅能够判断“是否允许访问”，还能够审计“是否按约交付”以及“异常发生后能否定位责任”。

同时，授权条款字段可根据医疗数据共享、金融授权查询和平台数据开放等场景扩展；由于本文采用条款摘要上链、条款明文链下保存的方式，新增字段不会显著增加链上存储压力。

3 实验与分析

3.1 实验目标与设置

本文主要从四个方面验证所提方法的有效性：一是验证三方授权条款的状态演化、一次性交付令牌和回执锚定机制能否形成完整闭环；二是评估在不同并发请求下的端到端时延与链上执行开销；三是分析在篡改、超期、重复调用和撤回后继续请求等异常条件下注入时，系统对异常交付的识别与阻断能力；四是结合误报率、鲁棒性和攻击模型，进一步分析所提机制在链下交付节点不完全可信条件下的稳定性与适用边界。

本文采用“联盟链节点+链下交付节点+分布式对象存储”的多主体部署环境。实验引入医疗数据协同、平台个人数据开放和金融授权查询三类典型业务场景模板，依据真实业务中的授权确认、用途限制、期限约束、撤回处理、交付回执和争议审计流程生成场景化请求。实验数据不包含可识别个人身份的真实明文，而是采用脱敏样例字段、公开数据结构和合成扩展数据相结合的方式生成，以兼顾场景真实性和个人信息保护要求。

为保证结果具有可比性，实验同时设置四类基线：静态访问控制列表方案（Static Access Control List，Static-ACL）、动态同意智能合约方案（Dynamic Consent Smart Contract，DynamicConsent-SC）[1-3]、基于去中心化身份的数据交易智能合约方案（DID-based Data Trading Smart Contract，DID-Trade-SC）[15-16]，以及在异常识别和追责分析中引入的可追溯访问控制方案（Traceable Access Control，Trace-AC）[18-19]。各方案在相同数据对象、请求负载、异常注入比例和并发压力下运行，并从功能正确性、授权激活时延、单次交付确认时延、异常交付识别率、误报率、端到端时延和可追责性等指标进行比较。系统配置如表 1 所示。

表 1 中的联盟链节点用于模拟个人数据流通场景中的多方协同与共同记账环境，主要承担条款注册、状态更新、条件校验、交付令牌签发和回执锚定等链上操作；链下交付节点用于模拟医院、平台企业或金融机构等数据持有方控制的数据交付服务，负责在验证一次性交付令牌后，从对象存储中读取并发送对应数据包；分布式对象存储用于模拟机构侧保存的个人数据资源。

表 1 系统实验配置

参数	取值
实验部署规模	12 个联盟链节点、8 个链下交付节点和分布式对象存储；联盟链节点采用 Ubuntu 22.04，16 vCPU，32 GB 内存；链下交付节点峰值发送速率为 50 MB/s
场景与数据对象	医疗数据协同、平台个人数据开放、金融授权查询三类场景模板；20 000 个数据对象，大小为 1 MB、5 MB、10 MB、50 MB 混合分布
条款、请求与并发	50 000 条授权条款实例，500 000 次请求事件；并发压力设置为 10、50、100、200、400 组请求
异常与评价指标	异常注入比例为 5%~25%，包含数据哈希不一致、超过有效期、额度耗尽后重复调用、授权撤回后继续请求四类异常；评价指标包括状态迁移正确性、时延、异常交付识别率、误报率和可追责性

数据对象规模为 20 000 个，既包含小型结构化记录，也包含中等规模文档和较大附件型数据，以覆盖不同交付负载。50 000 条授权条款实例用于模拟不同主体、数据对象、用途、期限和额度约束下的授权关系，500 000 次请求事件用于支撑后续功能验证、关键指标验证、并发性能分析以及异常识别实验。异常注入事件覆盖内容篡改、超期请求、越额重复调用和撤回后继续请求四类情况，后续将进一步结合误报率、鲁棒性和攻击模型分析所提方法的有效性与适用边界。

3.2 功能验证与关键指标

本文首先对三方授权条款驱动的自动交付流程进行功能验证。功能验证重点关注条款状态能否按照预期完成迁移、一次性交付令牌能否正确约束交付行为、交付回执能否重新锚定链上状态，以及异常交付是否能够触发拒绝、冻结或争议处理。实验设置五类典型场景：S1 为正常签署、激活与交付；S2 为个人在条款激活后撤回授权；S3 为交付节点返回版本不一致数据包；S4 为数据使用方在有效期外提交请求；S5 为额度耗尽后再次调用交付接口。各场景的触发条件与状态演化结果如表 2 所示。

由表 2 可以看出，本文方法在正常交付场景下能够完成从条款确认、条款激活到交付完成的闭环；在撤回、超期、版本不一致和重复调用等异常场景下，系统能够根据条款状态、有效期、额度、请求序号和数据哈希等约束条件进行拒绝或冻结处理。该结果说明，所提机制不仅能够完成授权状态记录，还能够将授权状态变化直接联动到后续数据交付资格，从而为异常阻断和责任追踪提供基础。

表 2　功能验证场景与状态演化结果

场景	测试目标	触发条件	预期状态演化	验证结果
S1 正常交付	验证授权生效、令牌签发与回执锚定闭环	三方签名有效，费用或外部条件满足，请求在有效期和额度内	Offer→Confirm→Active→Delivered	通过
S2 授权撤回	验证个人撤回授权后交付资格同步失效	个人在条款激活后发起撤回操作，使用方继续请求数据	Active→Revoke，并拒绝继续签发令牌	通过
S3 版本不一致	验证交付内容与条款登记版本的绑定关系	交付节点返回的数据包哈希或版本号与登记值不一致	Active→Dispute，并冻结同条款后续交付	通过
S4 超期请求	验证有效期约束与状态更新能力	使用方在授权有效期结束后提交交付请求	Active→Expire，并拒绝交付请求	通过
S5 重复调用	验证额度限制、请求序号和一次性令牌约束	额度耗尽后再次请求，或重复使用已消费令牌	拒绝请求或转入 Dispute，并记录异常日志	通过

在关键指标验证中，本文进一步比较不同方案在授权激活时延、单次交付确认时延、异常交付识别率、误报率和可追责性方面的差异。其中，异常交付识别率表示系统正确识别的异常事件占全部注入异常事件的比例；误报率表示正常交付请求被错误判定为异常的比例。不同方案的综合指标如表 3 所示。

表 3　不同方案关键指标比较

方案	激活时延/ms	交付确认时延/ms	异常识别率/%	误报率/%	可追责性
Static-ACL	46	63	29.8	0.8	弱
DynamicConsent-SC	76	116	63.5	3.9	中
DID-Trade-SC	103	151	71.2	4.6	中
Trace-AC	88	132	78.9	5.2	较强
本文方法	96	139	91.7	2.7	强

由表 3 可以看出，Static-ACL 方案由于只进行静态权限判断，授权激活和交付确认时延最低，误报率也较低，但其缺少对交付结果、版本一致性和重复调用的强约束，因此异常交付识别率较低。DynamicConsent-SC 能够支持授权更新与撤回，对异常请求具有一定识别能力，但由于缺少交付数据与条款版本之间的绑定，其异常识别能力仍然有限。DID-Trade-SC 强化了身份认证和交易授权，识别率有所提升，但链上验证步骤较多，导致时延增加。Trace-AC 引入了访问日志和可追溯记录，能够提升异常发现能力，但对正常请求中的边界状态变化更敏感，误报率相对较高。

相比之下，本文方法通过“条款地址-请求序号-一次性交付令牌-数据哈希-回执摘要”的多重绑定，将授权条件、交付动作和交付结果关联到同一条款实例中，因此在异常交付识别率上高于各对比方案。

3.3　并发性能分析

为评估系统并发处理能力，本文在 500 000 次请求事件中抽取不同并发压力进行端到端时延测试，并将并发请求数设置为 10、50、100、200 和 400 组。端到端时延从数据使用方提交交付请求开始计算，到交付节点完成数据发送且回执摘要被链上合约接收为止，主要包括身份校验、条款状态检查、一次性交付令牌签发、链下数据读取与发送、回执提交和状态更新等环节。各方案采用相同的数据对象分布、请求负载和异常注入比例，以保证实验结果可比。

由图 2 可以看出，随着并发请求数由 10 组提高到 400 组，各方案平均端到端时延均呈上升趋势。其中，Static-ACL 因仅进行静态权限判断而时延最低，但缺少对交付内容、次数和结果的约束；DID-Trade-SC 因身份验证和交易状态确认步骤较多，在高并发下时延增长最明显。本文方法的平均端到端时延整体高于 DynamicConsent-SC 和 Trace-AC，低于 DID-Trade-SC，在 10、50、100、200 和 400 组并发下分别为 116 ms、143 ms、190 ms、287 ms 和 425 ms。结果表明，一次性交付令牌、数据哈希校验和回执锚定会带来一定额外开销，但在 100 组并发以内仍可将时延控制在 200 ms 以内，能够满足多数低频、强约束的个人数据授权与交付业务需求。

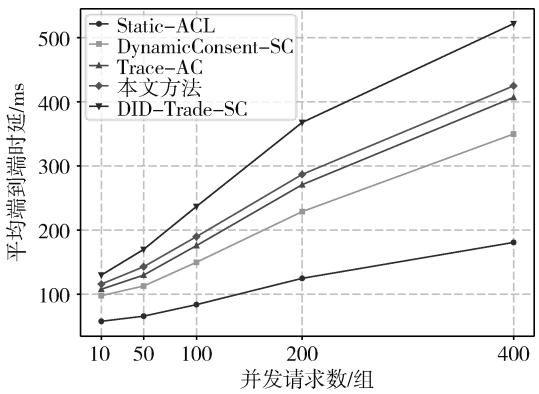

图 2　并发请求下不同方案的平均端到端时延

本文方法在高并发下的时延增长主要来自链上条款状态读取、令牌签发、回执状态更新，以及链下交付节点读取较大数据对象和生成回执的开销。由于本文仅将条款摘要、令牌状态和回执摘要写入链上，原始个人数据仍保留在链下，因此其增长幅度低于将身份解析、交易确认和状态验证集中到链上处理的 DID-Trade-SC。

3.4 异常交付识别与比较分析

为进一步检验可验证自动交付机制在异常场景下的有效性，本文在功能验证和关键指标统计的基础上，比较不同异常注入比例下各方案对异常交付行为的识别能力。实验设置 5%、10%、15%、20%和 25%五组异常注入比例，异常类型包括数据包哈希不一致、授权有效期外请求、额度耗尽后重复调用以及交付回执异常等。

图 3 给出了不同异常注入比例下的异常交付识别率。图中在 25%异常注入比例下，各方案的识别率分别为：Static-ACL 为 29.8%，DynamicConsent-SC 为 63.5%，DID-Trade-SC 为 71.2%，Trace-AC 为 78.9%，本文方法为 91.7%。其余注入比例下的数据按照相同实验流程统计得到，并保持随异常注入比例升高而递增的趋势。

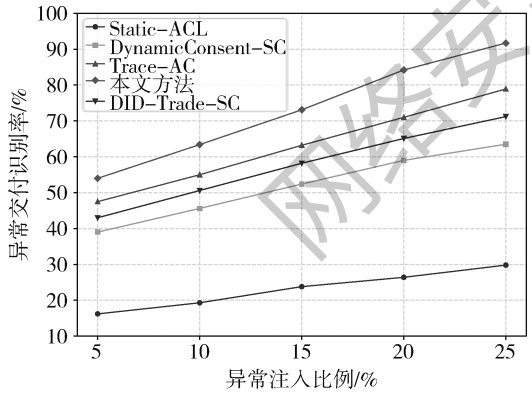

图 3　不同异常注入比例下的异常交付识别率

从整体趋势看，各方案的异常交付识别率均随着异常注入比例的提高而上升。这是因为异常事件占比增加后，系统能够观测到更多与条款状态、请求序号、令牌状态和交付结果不一致的样本，从而提升异常命中率。但不同方案的增长幅度存在明显差异。Static-ACL 主要依赖静态权限字段，只能识别未授权访问等显式异常，对交付内容是否符合条款缺少验证能力，因此识别率始终较低。DynamicConsent-SC 能够处理授权更新和撤回，但对交付数据版本、交付次数和回执结果的绑定不足，异常识别能力有所提升但仍受限制。Trace-AC 通过访问日志和追溯记录增强了异常发现能力，DID-Trade-SC 则通过身份可信绑定和交易状态记录提升了请求侧校验能力，因此二者整体优于 Static-ACL 和 DynamicConsent-SC。相比之下，本文方法将条款地址、请求序号、一次性交付令牌、数据哈希和回执摘要进行联合绑定，使异常检测不再仅依赖授权状态或访问日志，而是进一步覆盖交付触发、交付内容和交付结果三个环节。因此，在各组异常注入比例下，本文方法均保持最高识别率。

3.5 误报率、系统鲁棒性及攻击模型分析

为进一步评价所提机制的有效性，本文在异常交付识别率之外，引入误报率、攻击模型和系统鲁棒性进行分析。

从表 3 可以看出，Static-ACL 的误报率最低，为 0.8%，但异常交付识别率也最低，仅为 29.8%，说明其较少误拦正常请求的主要原因是约束能力不足。DynamicConsent-SC、DID-Trade-SC 和 Trace-AC 的异常识别率分别为 63.5%、71.2%和 78.9%，但误报率也分别升至 3.9%、4.6%和 5.2%，表明动态同意、身份增强和日志追溯机制虽然提升了异常发现能力，但在交付结果绑定和边界状态判断方面仍存在一定误判。相比之下，本文方法的异常交付识别率达到 91.7%，误报率为 2.7%，说明通过条款地址、请求序号、一次性交付令牌、数据哈希和回执摘要的多重绑定，可以在提高异常识别能力的同时保持较低误报率。

从鲁棒性看，本文方法可分别通过数据哈希和签名识别内容篡改，通过有效期和条款状态阻断超期请求，通过请求序号、nonce 和一次性令牌状态限制重复调用。因此，在链上状态、签名验证和哈希计算可信的前提下，本文方法能够对链下交付异常保持较稳定的识别能力。需要指出的是，本文机制主要约束交付阶段行为，对数据使用方获得数据后的线下二次传播、超范围分析等问题，仍需结合责任条款、日志审计、隐私计算或用途监管机制进一步处理。

在攻击模型方面，本文主要考虑三类交付阶段异常：一是内容篡改，即交付节点返回与条款登记版本不一致的数据包；二是超期请求，即数据使用方在授权期限届满后继续请求数据；三是重复调用，即在额度耗尽、令牌已使用或授权撤回后继续调用交付接口。本文不假设攻击者能够破解密码算法或控制联盟链多数节点，但允许链下交付节点存在延迟、故障、返回错误数据或重复响应等不完全可信情况。

4　结论

面向个人数据流通中授权表达不足、交付过程不可

验证和争议责任难界定等问题，本文提出了一种三方授权条款建模与可验证自动交付机制。该机制以数据持有方、个人和数据使用方为核心主体，构建覆盖主体域、数据域、约束域和责任域的授权条款模型，并通过去中心化身份、数字签名和智能合约实现条款注册、状态演化、令牌签发和回执锚定，从而形成“授权生效-条件校验-自动交付-结果验证-审计追责”的闭环。

实验结果表明，本文方法在引入条款校验、一次性交付令牌和回执锚定后，虽然带来一定额外时延，但整体开销仍处于可接受范围。与 Static-ACL、DynamicConsent-SC、DID-Trade-SC 和 Trace-AC 等方案相比，本文方法的异常交付识别率达到 91.7%，误报率控制在 2.7%，在异常识别能力、正常交付可用性和可追责性之间取得了较好平衡。并发实验和异常注入实验进一步表明，该机制能够较好识别数据篡改、超期请求和重复调用等交付阶段异常。

总体而言，本文方法适合作为个人数据共享、医疗数据协同和平台数据开放等场景中的上层授权治理与交付控制机制。后续工作将从三个方面展开：一是扩大真实场景和跨机构部署验证规模；二是与属性加密、可搜索加密、隐私计算和可信执行环境等技术结合；三是进一步引入违约量化、用途监管和形式化验证方法，提升条款执行和争议处置的自动化与可证明性。

参考文献

[1] Merlec M M, Lee Y K, Hong S P, et al. A smart contract-based dynamic consent management system for personal data usage under GDPR[J]. Sensors, 2021, 21(23): 7994.

[2] Peyrone N, Wichadakul D. A formal model for blockchain-based consent management in data sharing[J]. Journal of Logical and Algebraic Methods in Programming, 2023, 134: 100886.

[3] Daudén-Esmel C, Castellà-Roca J, Viejo A. Blockchain-based access control system for efficient and GDPR-compliant personal data management[J]. Computer Communications, 2024, 214: 67-87.

[4] Benchoufi M, Porcher R, Ravaud P. Blockchain protocols in clinical trials: transparency and traceability of consent[J]. F1000Research, 2017, 6: 66.

[5] Rantos K, Drosatos G, Demertzis K, et al. ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology[C]//Innovative Security Solutions for Information Technology and Communications. Cham: Springer, 2019: 300-313.

[6] Albalwy F, Brass A, Davies A. A blockchain-based dynamic consent architecture to support clinical genomic data sharing (ConsentChain): proof-of-concept study[J]. JMIR Medical Informatics, 2021, 9(11): e27816.

[7] Truong N B, Sun K, Guo Y. Blockchain-based personal data management: from fiction to solution[C]//2019 IEEE 18th International Symposium on Network Computing and Applications (NCA). Cambridge, MA, USA: IEEE, 2019: 1-8.

[8] Zyskind G, Nathan O, Pentland A. Decentralizing privacy: using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops. San Jose, CA, USA: IEEE, 2015: 180-184.

[9] Azaria A, Ekblaw A, Vieira T, et al. MedRec: using blockchain for medical data access and permission management[C]//2016 2nd International Conference on Open and Big Data. Vienna, Austria: IEEE, 2016: 25-30.

[10] 张磊, 郑志勇, 袁勇. 基于区块链的电子医疗病历可控共享模型[J]. 自动化学报, 2021, 47(9): 2143-2153.

[11] 牛淑芬, 陈俐霞, 李文婷, 等. 基于区块链的电子病历数据共享方案[J]. 自动化学报, 2022, 48(8): 2028-2038.

[12] 李亚红, 李强, 李哲玮, 等. 基于区块链且可验证完整性的电子病历数据共享方案[J]. 信息安全学报, 2025, 10(5): 129-139.

[13] 张正昊, 李勇, 张振江. 可控、可追责的敏感数据共享方案[J]. 计算机研究与发展, 2022, 59(12): 2750-2759.

[14] 张川, 王子豪, 梁晋文, 等. 面向跨联盟链的隐私保护数据要素交易审计方案[J]. 计算机研究与发展, 2024, 61(10): 2540-2553.

[15] 郝嘉琨, 向鹏, 何逸飞, 等. 基于去中心化身份的跨域数据交易系统[J]. 计算机研究与发展, 2024, 61(10): 2570-2586.

[16] 孟疏桐, 周铖鑫, 朱岩, 等. 一种智能法律合约驱动的联邦学习数据授权和执行方法[J]. 工程科学学报, 2026, 48(2): 331-345.

[17] 王有恒, 冯开开, 李汝佳, 等. 区块链智能合约隐私保护技术研究综述[J]. 计算机学报, 2025, 48(6): 1373-1416.

[18] 杜瑞忠, 刘妍, 田俊峰. 物联网中基于智能合约的访问控制方法[J]. 计算机研究与发展, 2019, 56(10): 2287-2298.

[19] 谢绒娜, 李晖, 史国振, 等. 基于区块链的可溯源访问控制机制[J]. 通信学报, 2020, 41(12): 82-93.

（收稿日期：2026-05-27）

作者简介：

吴超辉（1979-），男，博士，高级工程师，主要研究方向：数据治理。

高建彬（1976-），男，博士，副教授，主要研究方向：分布式智能、区块链技术、网络数据安全。

夏虎（1981-），通信作者，男，博士，副研究员，主要研究方向：分布式智能、数据治理。E-mail：xiahu@uestc.edu.cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部