面向个人数据要素化的可信授权系统设计

夏　虎[1]，吴志刚[2]，刘济铭[1]，尹国庆[3]，夏　琦[1]，高建彬[1]
（1. 电子科技大学　计算机科学与工程学院，四川　成都　611731；
2. 中国电子信息产业发展研究院，北京　100048；3. 66015 部队，北京　100192）

摘　要：针对个人数据要素化进程中用户权益保障不足、技术落地路径不清晰及通用性框架缺位三大核心问题，提出并构建了一个面向个人数据要素化的端到端可信授权技术框架。该框架整合去中心化身份、可验证凭证、零知识证明与智能合约等技术，形成覆盖授权-使用-计量-分账-审计全流程的闭环运行机制。框架以权属归户、管理自主、隐私保护、收益归户为设计目标，通过分层去中心化身份架构实现身份自主锚定与场景隔离，通过意图可验证凭证与字段级授权策略实现细粒度权限管控，通过链上计量与智能合约批量分账实现收益自动归户，通过零知识证明与同态加密实现数据可用不可见。基于开源工具构建的原型系统在典型数据使用场景中完成端到端功能验证，结果表明该框架能够实现分层身份管理、细粒度授权、隐私增强交付、链上计量与自动化分账等核心功能，全流程操作可上链存证并独立核验。成本评估显示，单次完整数据访问与分账流程的 Gas 消耗约为 158 万 Gas，经济成本可控。

关键词：数据要素化；个人数据；去中心化身份；可验证凭证
中图分类号：TP311　　**文献标志码：**A　　**DOI：**10. 19358/j. issn. 2097-1788. 2026. 07. 011

中文引用格式：夏虎，吴志刚，刘济铭，等. 面向个人数据要素化的可信授权系统设计[J]. 网络安全与数据治理，2026，45(7)：80-86.
英文引用格式：Xia Hu，Wu Zhigang，Liu Jiming. Design of a trusted authorization system for personal data factorization[J]. Cyber Security and Data Governance，2026，45(7)：80-86.

Design of a trusted authorization system for personal data factorization

Xia Hu[1]，Wu Zhigang[2]，Liu Jiming[1]，Yin Guoqing[3]，Xia Qi[1]，Gao Jianbin[1]
（1. School of Computer Science and Engineering，University of Electronic Science and Technology of China，Chengdu 611731，China；
2. China Electronics Information Industry Development Research Institute，Beijing 100048，China；3. Unit 66015，Beijing 100192，China）

Abstract：To address three core challenges in the process of personal data factorization—insufficient protection of data subjects′ rights and interests，unclear technical implementation paths，and the absence of a universal framework—this paper proposes and constructs an end-to-end trusted authorization framework for personal data factorization. The framework integrates existing technologies including decentralized identifiers，verifiable credentials，zero-knowledge proofs，and smart contracts，forming a closed-loop mechanism that covers the entire lifecycle of authorization，usage，metering，revenue distribution，and audit. Guided by the four design goals of ownership attribution，autonomous management，privacy preservation，and revenue attribution，the framework achieves identity autonomy and context isolation through a layered DID architecture，enables fine-grained permission control via intent-based verifiable credentials and field-level authorization policies，realizes automatic revenue attribution through on-chain metering and smart contract-based batch distribution，and ensures data usability without plaintext exposure by leveraging zero-knowledge proofs and homomorphic encryption. A prototype system built on open-source tools has been functionally validated in typical data usage scenarios. The results demonstrate that the framework supports layered identity management，fine-grained authorization，privacy-preserving data delivery，on-chain metering，and automated batch distribution，with all critical operations recorded on-chain and independently verifiable. The cost evaluation demonstrates that the gas consumption for a single complete data access and revenue-splitting process is estimated to 1. 58 million gas，indicating that the economic cost is manageable.

Key words：data factorization；personal data；decentralized identity；verifiable credential

0 引言

数据作为新型生产要素，是数字经济发展的核心战略资源。2022 年《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》明确提出建立保障权益、合规使用的数据产权制度[1]。然而在个人数据要素化进程中，个人作为原始数据的核心贡献者，长期面临控制权缺失、收益分配缺位、授权机制形式化等问题，形成“贡献者无权、使用者无责”的结构性矛盾[2]。当前个人数据权益治理存在三大现实困境：一是权益保障困境，以 GDPR 为代表的事后监管模式及国内中心化平台授权模式，均难以实现数据主体对自身数据的实时管控与权益落地[3-4]；二是技术离散困境，现有研究在授权、使用、计量、分账、审计等单一环节虽有探索（如身份与授权[5-6]、隐私计算[7-8]、智能合约计量[9-10]、审计存证[11]），但未形成全流程互操作的闭环方案；三是通用框架缺位，已有方案多面向特定场景，缺乏标准化、可复用的系统级技术架构。

在理论研究层面，数据产权已从“所有权归属”转向“权利束分离”范式，主张分离控制权与使用权，并细化为访问权、收益分享权等可执行子权利[2,12-13]；“数据主权”与“个人信息自决权”强调数据主体的自主控制能力[14]，“动态同意”机制倡导细粒度授权[15]，但这些研究多停留在制度建构层面，缺乏从法律赋权到技术执行的完整转化路径。在技术实现层面，去中心化身份（Decentralized Identity，DID）[6]、零知识证明（Zero-Knowledge Proof，ZKP）[7]、智能合约[10]等技术为局部环节提供了支撑，但各模块缺少统一身份锚点、互操作授权机制与可衔接的计量分账逻辑，难以支撑规模化落地。

为此，本文整合去中心化身份、可验证凭证（VC）、零知识证明、智能合约等技术，构建面向个人数据要素化的端到端可信授权框架。框架确立“权属归户、管理自主、隐私保护、收益归户”四大目标，设计覆盖“授权-使用-计量-分账-审计”全流程的闭环运行机制，并基于开源工具栈实现原型系统，验证其功能完整性与经济可行性，为个人数据要素化提供可复用的系统级解决方案。

1 系统总体架构设计

1.1 架构设计目标与原则

1.1.1 架构设计目标

针对个人数据要素化中的四类核心问题，系统确立以下设计目标：

（1）权属归户：通过去中心化身份建立数据与主体的密码学绑定，确保每份数据可唯一归属于一个数据主体。

（2）管理自主：构建用户可配置、可撤销的细粒度授权机制，实现访问权限的全生命周期自主控制。

（3）隐私保护：融合零知识证明与同态加密（Homomorphic Encryption，HE）技术，使数据使用方仅能获知验证结果（是/否）或计算结果，而无法获取原始数据。

（4）收益归户：基于智能合约实现按次累加、自动执行的收益分配，去除中间截留环节。

1.1.2 架构设计原则

为确保系统的安全性、可扩展性与工程可行性，架构设计遵循以下五项核心原则：

（1）分层解耦原则。采用三层递进式架构（价值目标层-核心功能层-技术支撑层），各层职责明确、边界清晰，通过标准化接口实现层间解耦与协同，以降低模块耦合度，支持技术迭代与多场景扩展。

（2）区块链原生原则。以区块链为信任基础设施，将身份注册、授权签发、使用计量、收益分账、操作审计等核心状态上链存证，依托不可篡改、可追溯、透明可验证的技术特性，构建去中心化的信任锚点。

（3）标准兼容原则。严格遵循 W3C 发布的去中心化身份（DID）与可验证凭证（VC）国际标准，保障系统的互操作性与通用性，以适应多元场景下的数据要素流通需求。

（4）隐私优先原则。将隐私保护贯穿架构全生命周期，从身份隔离、授权约束到数据使用环节，全链路嵌入零知识证明、同态加密等隐私增强技术，在合规性与可用性之间实现可配置的平衡。

（5）可审计可监管原则。构建端到端的审计追溯机制，为监管机构提供独立的核验入口，实现“技术自治”与“合规监管”的协同治理，满足数据要素市场的可监管性要求。

1.2 三层递进式总体架构

基于前述设计目标与原则，本文构建了一个“价值目标-核心功能-技术支撑”的三层递进式架构，如图 1 所示。该架构以价值目标为顶层纲领，以核心功能为业务载体，以区块链技术为底层信任基础设施，形成从制度要求到技术实现的可映射、可落地、可验证的完整链路。

1.2.1 价值目标层

价值目标层是架构的最高抽象层次，明确了系统

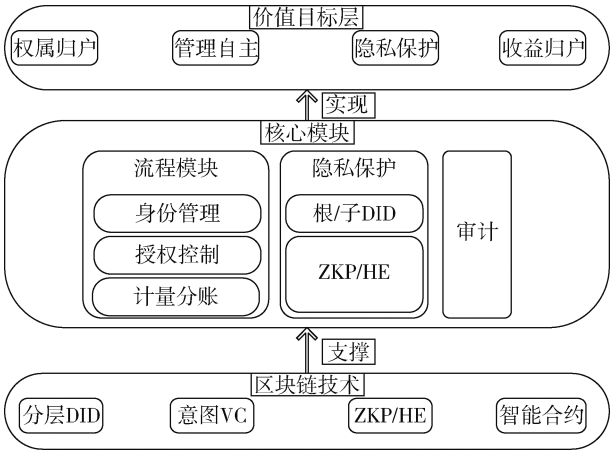

图 1　总体架构图

应实现的核心价值导向，并为下层功能与技术的设计提供约束与评判依据。该层包含四项互相关联的设计目标：权属归户、管理自主、隐私保护与收益归户。它们分别对应于个人数据要素化过程中数据主体的身份确权、控制权行使、安全保护与价值分配四项基本权益。通过将上述制度层面的权利主张转化为可量度、可验证的技术目标，该层从顶层锚定了“以人为本”的设计理念，确保后续所有技术实现均围绕数据主体权益展开。

1.2.2　核心功能层

核心功能层是架构的业务执行主体，负责将价值目标转化为可操作、可协同的功能模块。该层由五大功能模块构成——身份管理、授权控制、隐私保护、计量分账与审计追溯，它们以闭环方式覆盖个人数据从身份确权到价值分配的全生命周期。

身份管理模块是系统的信任根基。该模块基于W3C DID 标准，构建“根 DID+角色化子 DID”的分层身份体系。根 DID 作为数据主体全局唯一、永久有效的身份锚点，通过密码学签名与个人数据资产建立强绑定关系，实现数据权属的可验证确权；子 DID 由根 DID 派生，面向不同业务场景独立生成，实现场景间的身份隔离，从源头上防范跨场景关联追踪。该模块同时承担可验证凭证的签发、存储、验证与状态管理，为授权、访问、分账等环节提供标准化信任载体。

授权控制模块是数据访问权限的全生命周期管控核心。该模块引入意图驱动的细粒度授权机制：数据需求方以其子 DID 发起包含数据对象、使用目的、使用期限、访问范围等要素的标准化使用意图，并将意图封装为可验证凭证上链存证。数据主体基于该意图凭证配置字段级访问限制、有效期限、访问次数及分账规则等多维授权策略，经链上匹配校验后由数据主体签名上链，形成不可篡改的授权依据。在数据访问阶段，系统自动对意图凭证、授权策略及其撤销状态进行链上校验；数据主体可随时发起授权撤销操作，从而实现权限的动态管控与全程自主可控。

隐私保护模块是数据安全的核心保障。该模块融合多种隐私增强技术：以零知识证明为核心，使数据主体能在不披露原始数据的前提下向需求方证明特定属性成立，满足最小信息披露原则；辅以同态加密技术，支持对密文数据的直接计算，实现“数据可用不可见”；同时依托分层 DID 的身份隔离机制，阻断不同场景下的身份关联，从身份与数据两个维度共同保障隐私安全。

计量分账模块是数据价值分配的执行载体。每次合法数据访问行为触发链上计量事件，由智能合约自动记录访问主体、数据类型、访问时间、使用频次等信息，生成不可篡改的计量凭证。基于授权阶段预设的分账规则，智能合约自动完成收益核算、划转与上链存证，形成“使用即计量、计量即分账、分账即到账”的自动化执行链条，去除中心化平台的中转环节，确保数据价值直接归属于数据主体。

审计追溯模块是系统的可信监管支撑。该模块将身份创建、授权签发、权限变更、数据访问、计量分账、授权撤销等所有关键操作以结构化事件日志形式上链存储，形成连续、完整、不可篡改的操作轨迹。数据主体、需求方及监管机构均可独立核验上述日志，无需依赖第三方平台即可验证授权合法性、使用合规性与分账准确性，从而为纠纷处理、合规检查与责任认定提供强信任技术基础。

1.2.3　区块链技术支撑层

区块链技术支撑层是架构的底层信任基础设施，为上层核心功能提供去中心化、不可篡改、可验证的执行环境。具体而言，分层 DID 机制支撑身份管理模块的根/子 DID 体系，实现身份自主创建、权属绑定与场景隔离；可验证凭证承载授权策略与使用意图，为授权控制模块提供标准化、可撤销的信任载体；零知识证明与同态加密为隐私保护模块提供核心密码学原语；智能合约则承载授权校验、链上计量、自动分账与状态管理等关键逻辑，确保系统规则的自动化、不可篡改执行，并为审计追溯模块提供链上存证的执行基础。

1.3　架构协同机制

三层架构之间形成“目标约束–功能承载–技术支撑”的双向闭环关系。价值目标层为核心功能层提供

设计约束与评判依据，核心功能层向技术支撑层提出能力需求，技术支撑层通过标准化接口向上提供服务。同时，核心功能层的运行结果可反向验证价值目标的达成程度，形成设计、实现与验证的闭环迭代。

五大功能模块之间的协同关系可概括为相互依赖、彼此约束的有机整体。表 1 总结了各模块之间的依赖方向与约束关系。

表 1　功能模块间的依赖关系

依赖模块	被依赖模块	依赖内容
授权控制	身份管理	需验证请求方与被授权方的 DID 身份
隐私保护	授权控制	需在授权策略定义的边界内执行计算
计量分账	授权控制	需依据授权策略中的分账规则进行分配
计量分账	隐私保护	需以合法访问事件为触发条件
审计追溯	全部其他模块	需接收所有模块的操作日志

具体而言，身份管理模块为全系统提供统一的身份锚点，是其他所有模块运行的前提；授权控制模块输出的授权策略，同时约束隐私保护模块的计算边界与计量分账模块的分配规则；隐私保护模块在授权框架内保障数据使用过程的安全性；计量分账模块依据授权规则完成价值分配；审计追溯模块则接收前述四个模块的操作日志，维护全局不可篡改的审计链。上述链式依赖关系，使得任一数据访问请求的合法性可分解为身份认证、授权校验、安全计算、计量记录与日志存证五个可独立验证的子条件。

在上述协同机制中，一项关键的设计原则是职责分离：身份管理模块仅负责 DID 的生成、解析与凭证状态维护，不参与授权判定；授权控制模块仅依据链上策略执行校验，不干预数据内容的计算；隐私保护模块仅在授权边界内执行密码学运算，不涉及收益分配。各模块通过标准化接口进行交互，实现功能内聚与接口隔离，在保障协同效率的同时支持各模块的独立迭代。

1.4　与代表性方案的对比分析

为明确本文架构的设计定位，选取三类代表性方案进行定性对比：（1）中心化授权平台（以 OAuth 2.0 及主流互联网开放平台为典型）；（2）去中心化数据市场（以 Ocean Protocol、DataBroker DAO 为代表）；（3）去中心化身份/可验证凭证框架（以 Veramo、Hyperledger Aries 为典型）。对比维度涵盖身份模型、授权粒度、隐私保护、收益分账、审计方式与互操作性，结果如表 2 所示。

表 2　与代表性方案的架构对比

维度	中心化平台	去中心化数据市场	DID/VC 框架	本文架构
身份模型	平台托管账户	钱包地址	W3C DID	根 DID +子 DID
授权粒度	应用级	资产级	VC 声明级	意图 VC +字段级
隐私保护	平台可见明文	链上透明	依赖外部	内嵌 ZKP +HE+隔离
收益分账	平台截留	合约分账	不涉及	合约批量分账
审计方式	平台日志	链上交易	VC 状态	全流程链上
互操作性	平台封闭，跨平台不通	基于链标准，中等互通	遵循 W3C 标准，通用性强	兼容 W3C DID/VC 标准

对比表明，本文架构在细粒度授权、原生隐私保护与自动化批量分账方面实现了有机融合，弥补了中心化平台、去中心化数据市场及传统 DID/VC 框架各自的短板。

2　核心工作流程

2.1　流程概述

面向个人数据要素化全生命周期可信流转需求，本文基于所提三层架构，设计一套覆盖需求匹配、数据交付、计量分账与审计追溯的端到端闭环工作流程。流程以去中心化身份为信任锚点、以可验证凭证为授权载体、以区块链智能合约为执行引擎，在完成授权策略与使用请求的可信匹配后，通过隐私增强技术实现安全数据交付，并依据数据实际使用量执行自动化批量分账，最终实现全流程操作上链存证与可追溯验证。整套流程严格遵循“权属归户、管理自主、隐私保护、收益归户”的设计目标，将数据授权、使用、分配、监管融为一体，形成技术可执行、权益可保障、过程可监管的标准化运行机制。

2.2　需求匹配阶段

需求匹配阶段以数据需求方的使用请求为输入，以生效的意图可验证凭证为输出。该阶段的完整流程如图 2 所示。

数据需求方首先以其子 DID 发起数据使用请求，请求中明确数据范围、使用目的、使用期限及访问频率约束。系统将该请求封装为意图可验证凭证，并将其哈希值上链存证，从而保证意图的不可篡改性与不可抵赖性。

数据提供方收到意图可验证凭证后，依据预置的授权策略进行校验。授权策略以可验证凭证形式表达，包含字段级访问权限、有效期、单日访问上限及分账单价等约束。校验过程主要考察三项条件，即请求的

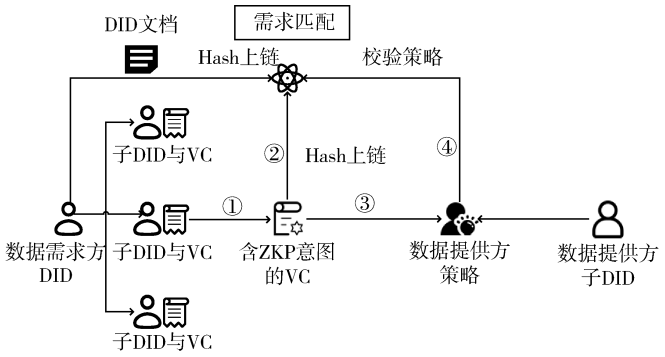

图 2　需求匹配流程图

数据范围是否在授权范围内，使用目的是否被允许，以及使用期限与访问频率是否满足上限要求。若上述条件全部满足，智能合约将意图可验证凭证与授权策略的匹配关系上链，该凭证正式生效，成为后续数据访问的唯一合法依据。若任一条件不满足，请求即被终止，终止事件同时上链存证。该阶段的关键在于授权关系的建立不依赖任何第三方，且所有状态变更均可公开验证。

2.3　数据交付阶段

授权生效后，流程进入数据交付阶段。该阶段的输入为生效的意图可验证凭证及对应的原始数据，输出为数据需求方所需的结果，该结果可以是布尔值或计算结果。系统根据授权策略中指定的使用目的自动选择以下两条路径之一执行，整体交付流程如图 3 所示。

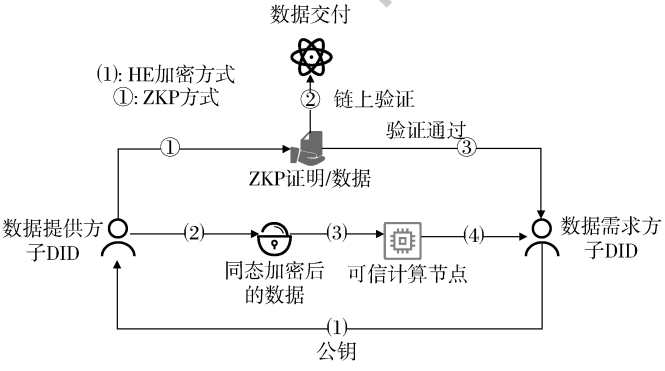

图 3　数据交付流程图

第一条路径为属性验证路径，适用于属性核验类场景，例如年龄验证或信用评分判定。在该路径中，数据提供方针对待验证属性生成零知识证明，并提交至链上验证合约。验证合约在不获取原始数据的前提下判定证明的有效性，随后仅向数据需求方返回通过或拒绝的结果。该路径的输出不包含任何原始数据。

第二条路径为数据计算路径，适用于数据计算类场景，例如统计、聚合。在该路径中，数据需求方预先向数据提供方发送公钥。数据提供方使用该公钥对原始数据进行同态加密，并将密文发送至可信计算节点。可信计算节点在密文状态下执行预设计算任务，最终仅将计算结果返回给数据需求方。该路径中原始数据始终以密文形式存在，需求方无法接触原始数据。

两条路径互斥执行，路径选择由授权策略中的使用目的字段决定，且对数据提供方透明。

2.4　计量分账与审计追溯阶段

数据交付完成后，流程进入价值回流阶段。该阶段依次执行计量、分账与审计三项操作，三者顺序执行且相互依赖。

在计量环节，每次数据交付触发链上计量事件。智能合约记录访问主体、数据对象、时间戳及交付路径类型，并生成不可篡改的计量凭证。该凭证是后续分账的唯一输入依据。

在分账环节，智能合约依据授权策略中预设的分账规则，对同一数据提供方且同一授权策略下的计量凭证进行汇总，自动完成收益核算，并将代币直接划转至数据提供方子 DID 账户。整个分账过程不涉及人工干预，划转记录同时上链存证。

在审计环节，从身份创建、授权签发、策略变更到数据交付、计量记录、分账执行，所有关键操作均以结构化事件日志形式上链存储。数据提供方、数据需求方及监管机构均可独立核验操作日志，从而验证授权合法性、使用合规性与分账准确性。

3　系统实现与评估

本节详细阐述所提框架的原型系统实现方案，并从经济成本与功能完备性两个维度对系统进行评估。原型系统以开源技术栈为基础，实现了身份管理、授权控制、隐私保护、计量分账及审计追溯五大核心模块，并针对典型数据使用场景完成了端到端功能验证与 Gas 消耗实测。

3.1　原型系统实现

为验证所提框架的可行性，本文基于开源技术栈搭建模块化原型系统，依托区块链底层支撑，落地身份管理、授权控制、隐私保护、计量分账、审计追溯五大核心功能，实现个人数据全流程可信流转与权益自主保障。

身份管理层面，系统遵循 W3C 标准，搭建根 DID+场景化子 DID 分层身份架构，并引入意图 VC 与

授权策略 VC 两类标准化凭证，结合链上哈希存证，实现细粒度、可撤销、可核验的自主授权管控。

合约层面部署五类核心智能合约，分别对应身份管理、授权校验、隐私证明存证、数据审计、批量分账功能。各合约协同联动，自动完成身份核验、授权匹配、行为记录与收益划转，依靠区块链不可篡改特性，实现全流程去中心化可信执行。

隐私保护层面，系统构建零知识证明+同态加密双路径隐私交付体系，适配不同数据使用场景。属性核验场景采用零知识证明，无原始数据泄露；数据聚合计算场景采用同态加密密文运算，全程保障数据可用不可见，平衡数据可用性与隐私安全性。

业务层面实现数据申请、隐私交付、批量分账、链上审计的全闭环自动化运行。系统依据预设规则自动聚合数据使用记录、核算分配收益，消除中心化截留问题，保障数据收益归户。所有操作全程上链存证，可独立追溯核验，满足合规监管需求。

原型系统部署于无 Gas 消耗的 Tinc 可信链网，运行成本极低。为量化系统开销、适配主流区块链生态，本文在以太坊兼容测试环境中复现核心逻辑并完成 Gas 消耗测试，为框架规模化落地提供量化支撑。

3.2 成本评估

如 3.1 节所述，本文原型系统实际部署在 Tinc 区块链上，该链不消耗 Gas，因此无直接的经济成本。但为了量化各操作的计算资源开销，并为本框架迁移至其他公链或联盟链提供参考，本文在一台本地搭建的以太坊兼容测试网络上，使用 Solidity 0.8.19 实现了相同的智能合约逻辑，并测量了各核心操作的 Gas 消耗。需要说明的是，以下 Gas 数据仅代表测试环境下的计算资源消耗量，Tinc 链上实际业务运行时不产生 Gas 费用；若将本框架部署至其他采用 Gas 计费的区块链，则需参考下述数值评估成本。

3.2.1 合约部署成本

五类核心合约的部署 Gas 消耗如表 3 所示，总部署成本约 494 万 Gas，该成本为一次性开销。

表 3　合约部署 Gas 消耗

合约名称	Gas 消耗	占比/%
DIDManager	1 094 765	22.2
AuthorizationPolicy	1 015 519	20.5
DataUsageAudit	770 065	15.6
RevenueDistribution	1 008 237	20.4
ZKPProofRegistry	1 054 214	21.3
合计	4 942 800	100

3.2.2 完整流程 Gas 消耗

基于实测值，单次完整数据访问与分账流程的 Gas 消耗如表 4 所示。

表 4　写操作 Gas 消耗

步骤	Gas 消耗
创建根 DID	142 950
创建子 DID	187 846
策略创建	279 044
审计记录	235 818
ZKP 证明上传	277 834
批量分账	455 417
合计	1 578 909

需要说明的是，上述流程中的多项操作具有可复用性，其 Gas 消耗经多次分摊后可显著降低。在本框架的实际部署环境——Tinc 区块链中，由于平台设计上不消耗 Gas，所有操作的实际运行成本为零。即使迁移至其他采用 Gas 计费的联盟链，Gas 价格通常也可设为零或极低固定值，实际成本依然可忽略不计。因此，本文框架在经济层面具备充分的可行性。

3.3 功能验证

基于自动化测试，本文原型系统在典型数据授权使用场景下完成了端到端逻辑验证，所有核心功能均已通过：分层 DID 体系支持 Ed25519 密钥对与 did:key 标识符生成、子 DID 确定性派生，并可生成符合 W3C 规范的身份文档；意图 VC 与授权策略 VC 实现签发、哈希验证与生命周期管理；授权策略支持字段级权限及每日访问上限；ZKP 路径的公开输入仅含断言结果与数据指纹，HE 路径在 Paillier 密文上完成同态加法并解密正确；数据市场支持发布、浏览、一键请求及审批（非所有者请求被拒绝），审批时自动完成支付结算（请求方扣款、数据所有者增收）；批量分账按策略分组生成含付款方信息的收益记录；交易历史支持双视角查询；全流程上链存证，审计日志覆盖身份、策略、访问、隐私计算与收益分配关键环节；链上服务不可用时支持降级至本地存证并确保最终一致性。

综上，框架在功能逻辑层面完备且可运行，支撑从身份确权、授权管控、隐私交付到价值回流的端到端闭环交易，但当前验证基于模拟环境与自动化用例，尚未进行大规模分布式压力测试与性能评估，相关工作留待后续研究。

4 结论

针对个人数据要素化进程中用户权益保障不足、

授权管控薄弱、隐私易泄露及收益分配机制缺失等突出问题，本文设计并实现了一种以人为本的数据要素可信授权系统。系统以“权属归户、管理自主、隐私保护、收益归户”为核心设计目标，采用“价值目标层-核心功能层-区块链技术支撑层”的三层递进式架构，整合去中心化身份、可验证凭证、零知识证明及智能合约等现有技术，构建了覆盖“授权-使用-计量-分账-审计”全流程的闭环运行机制，实现了个人数据从身份确权、权限控制、隐私交付到价值回流的可信、自主、安全流转。

原型系统的实现与功能验证结果表明，所提框架能够有效支撑分层 DID 身份管理、意图驱动的细粒度授权、基于零知识证明与同态加密的隐私增强数据交付、链上计量与自动化批量分账等核心功能。全流程关键操作均可上链存证并实现独立核验，具备良好的可审计性与可监管性。成本评估显示，单次完整数据访问与分账流程的 Gas 开销约为 158 万 Gas，经济成本可控，具备实际部署的可行性。

在用户密钥管理方面，当前原型系统要求用户自行保管根 DID 私钥，未内置恢复机制，这是去中心化身份体系在用户体验层面的普遍挑战，留待后续工程化工作解决。

本研究为个人数据要素化提供了一套标准化、可复用、可落地的系统级技术方案，也为数据主体权益的可验证、可执行保障提供了可行的技术路径。当前系统仍存在若干有待优化之处：在合规层面，智能合约授权机制与现行法律法规的深度适配尚需进一步完善；在性能层面，零知识证明生成与链上交互效率仍有提升空间；在工程层面，用户密钥管理与交互体验仍需优化。未来工作将围绕合规合约化、跨链互操作、轻量化隐私计算及易用性交互设计等方向展开，推动系统在医疗、金融、公共服务等多场景中的实际落地应用，为数据要素市场的高质量发展与数据主体权益的全面保障提供更坚实的技术支撑。

参考文献

[1] 中共中央，国务院. 关于构建数据基础制度更好发挥数据要素作用的意见[Z]. 2022.

[2] 杨翱宇. 数据财产权益的归属判定[J]. 重庆大学学报(社会科学版),2023,29(1):241-254.

[3] Kalsi M. Still losing the race with technology? Understanding the scope of data controllers′ responsibility to implement data protection by design and by default[J]. International Review of Law Computers & Technology, 2024, 38(3): 346-368.

[4] Chen Yiming, Liu Liming, Deng Jinpei. Governing data through privacy after China′s PIPL: discursive strategies, layered compliance and power dynamics in digital platform policies[J]. Telecommunications Policy, 2025,50(3): 103147.

[5] Chockalingam S, Pirbhulal S, Abie H. Improving security and privacy of cognitive digital twins through dynamic consent for healthcare and resilient societies[C]//International Conference on Human-Computer Interaction. Cham: Springer Nature Switzerland, 2025: 293-305.

[6] Mazzocca C, Acar A, Uluagac S, et al. A survey on decentralized identifiers and verifiable credentials[J]. IEEE Communications Surveys & Tutorials, 2025,27(6):3641-3671.

[7] Namazi M, Nemecek A, Ayday E. ZKPROV: a zero-knowledge approach to dataset provenance for large language models[J]. arXiv preprint arXiv:2506. 20915, 2025.

[8] 胡鹏，孙磊，胡翠云，等. 面向深度学习的高效安全推理研究综述[J]. 通信学报，2025，46(5)：238-257.

[9] Bauer-Hänsel I, Liu Q, Tessone C J, et al. Designing a blockchain-based data market and pricing data to optimize data trading and welfare[J]. International Journal of Electronic Commerce, 2024, 28(1): 3-30.

[10] 唐经纬，王玲芳，李杨. 基于智能合约的细粒度数据交易计量验证方法[J]. 电子设计工程，2024，32(9)：1-5.

[11] Gao Lixia. Enterprise internal audit data encryption based on blockchain technology [J]. PLOS One, 2025, 20(1): e0315759.

[12] Filatova-Bilous N. Data as a tradeable commodity: propertization vs. the concept of exclusive rights[J]. Teisė, 2022, 124: 55-66.

[13] 孔德明. 数据财产权到访问权:欧盟数据设权立法转型解析[J]. 比较法研究，2023(6)：33-50.

[14] 夏伟. 数字时代个人信息“真实自决权”的法治回归[J]. 学术界，2026(1)：167-178.

[15] 夏庆锋，戴媛媛. 个人信息处理同意规则的动态场景化完善[J]. 安徽大学学报(哲学社会科学版)，2025，49(5)：113-122.

（收稿日期：2026-05-25）

作者简介：

夏虎（1981-），男，副研究员，主要研究方向：分布式智能、数据治理。

吴志刚（1969-），男，正高级工程师，主要研究方向：数据治理。

高建彬（1976-），通信作者，男，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。E-mail：gaojb@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