数据交易PDCA模型

The PDCA Model for Data Transactions

合肥工业大学

上海数据交易所

版权声明

编写组（排名不分先后）

刘业政、姜元春、蔡浴泓、薛立德、柴一栋、孙见山、
孙春华、袁昆、钱洋、宗兰芳、周芦娟、金斗。

编写单位（排名不分先后）

合肥工业大学
上海数据交易所

目录
Contents

报告要点

数据作为数字经济的核心生产要素和创新动力源泉，蕴含着事物的关联性及其发展规律，对提升国家安全管理能力、社会治理能力、经济发展质量等各方面具有重要的价值。然而，数据要素流通使用环境复杂，承载多方主体利益，流通使用过程环节众多，容易引发多重安全风险和隐私泄露问题，威胁个人隐私、商业秘密、国家安全以及各参与主体的合法权益，严重制约数据要素大规模流通使用。近年来，政府组织、学术界和产业界围绕数据要素在产权分配、数据治理和数据资产等方面的问题，很少有研究在中观或者微观层面关注数据流通交易、数据市场可持续发展的基础条件——市场信任。

由于数据要素市场的双向信息不对称性，供需双方存在信任壁垒问题一方面导致了供需双方对另一方道德风险和资质风险的感知，降低其市场参与的信心，另一方面导致参与主体间高昂的信任沟通成本，降低了市场运行效率。建立数据要素市场可信生态，构建诚实、守信和公平的营商环境不仅可以避免“劣币驱逐良币”，还可以促进数据要素市场的可持续发展。因此，构建数据要素流通使用的信任理论基础，建立数据要素流通使用全过程合规信任机制，对破解数据要素市场信任壁垒，促进数据要素高效流通使用、推动数据要素市场化配置、健全完善数据要素市场、加快数据要素价值释放具有重要意义。

本报告以数据要素如何高效可信流通使用为主线，综述了数据要素可信流通使用理论与方法。首先辨析了信任的概念和相关理论，界定了数据要素可流通交易信任的概念,并通过文献调研，对数据要素流通交易中的关键主体、关键客体和流通环境进行风险识别分析。综上，本报告面向数据要素流通交易过程涉及道德关键主体和客体，提出了 PDCA 可信模型，即主体可信（Participant）、数据可信（Data）、合约可信（Contract）和算法可信（Algorithm）。其依据数据要素流通交易全流程可信的要求，即事前审查阶段需要保障主体资质可信、数据质量可信和合约内容可信，在事中监控阶段要保障主体行为和算法行为可信，在事后审计阶段，要对数据流通使用过程进行追溯，更新主体和数据的信用评估。此外，本报告还给出了基于 PDCA 模型的数据可信流通交易评估指标和测度体系，以及数据交易 PDCA 可信模型的实现路径和保障体系。

一、前言

近年来，随着我国一系列政策的出台，数据要素市场建设已经取得了重要进展，也受到了国内外学者和业界的广泛关注。这些关注主要是在产权分配、数据治理和数据资产等方面，很少有研究在中观或者微观层面关注数据流通交易、数据市场可持续发展的基础条件—市场信任。

1.1 数据要素流通交易中建立信任机制的意义

数据要素的可信流通使用是数字经济可持续发展的客观要求。数字经济即将进入创新发展阶段，促进高质量数据要素供给、流通以及开发利用，实现数据要素流通和利用的制度创新是数字经济高质量发展的内在要求[1]。数据作为新型生产要素，只有经过市场可信流通，才能彰显数据要素的价值，实现数据产品化[2]。另外，推动数据要素在国际上的可信流通，可以进一步引领全球化数字经济的发展[3]。

数据要素的可信流通使用是破解主体间信任壁垒，提高市场运行效率的重要举措。在数据要素市场，供需双方存在信任壁垒问题，深层次的原因在于：供需双方对数据价值的双向不确定性，在传统商品中，一般来讲产品的价值决定了产品的价格，但是数据产品的价值检验和产品使用是重叠的，供需双方都无法确定数据产品相对于对方的价值[4]。现有研究关注较多的另一个问题是数据使用过程中的不可证实性，数据供方无法得知自己的数据将被如何使用以及数据需方是否具有数据保护的能力，数据需方也很难向第三方证实自己是否滥用了供方数据[5]。这种信息不对称性和不可证实性所导致的问题是供需双方对对方道德风险和资质风险的感知，一方面降低了其市场参与的信心，另一方面参与主体间存在高昂的信任沟通成本，降低了市场运行效率。

数据要素的可信流通使用是促进数字产业与传统产业融合的有效途径。数据要素作为一种新兴生产要素，只有与传统要素相结合才能更好的发挥价值[6]。而当前主要存在的问题是除了传统企业在进行数字化转型方面的动力不足，数据要素的供给和流通还缺乏成熟的服务生态。一方面，数据要素市场缺乏成熟的数商生态，同时传统的中小企业很少具备专业的数据治理能力和数据管理意识。因此，数据资源向数据产品转化成本较高，市场供给动力不足。另一方面，第三方数据交易机构与传统企业在发展中的协调程度不高，中小企业对数据价值认知不足，无法准确描述数据产品需求，亟需数据交易平台搭建双边市场，提供智能匹配和数据推荐服务。通过专业的数据处理服务、精准的供需匹配和细心的数据管理辅导等方式实现数据产品的可信流通使用，才能促进传统产业与数字产业的深入结合以及协同创新。

数据要素的可信流通使用是合规高效释放数据要素潜在价值的核心引擎。数据要素的可信流通并不是单方面保证数据流通使用的安全，而是兼顾隐私保护、数据安全和数据流通使用效率。随着算法技术的不断发展，不断衍生出更多种类、更加智能的数据加工及处理服务，以透过数据发现知识。但是算法本身是一个“黑匣子”，很难检测算法是否安全合规、公平透明。目前学术界已经致力于解决 AI 算法的治理问题，例如关于算法的安全性[7]、公平性[8]和可解释性[9]等算法要求受到国内外学者越来越多的关注。因此，实现数据要素的可信使用才能促进释放数据要素价值，推动产业数据流通。

1.2 国内外数据要素流通交易信任机制的研究现状

2022 年我国数据产量达 8.1ZB，同比增长 22.7%，数据要素市场的交易规模得到明显提升，构建数据要素的可信流通交易体系已经成为数据要素市场未来发展的方向。面向数据要素流通的关键节点，构建数据要素流通使用的可信模型及评估方法，为建立数据要素可信生态体系提供理论基础，是当前数据治理研究中的重点目标。然而数据要素市场涉及多级数据产品、多元市场主体以及多种交易方式对我们认识数据要素可信流通的本质特征和内在逻辑带来了巨大的挑战。不同区域、不同机构的数据管理制度、数据交易规范和数据治理技术相互割裂，对实现全国一体化的数据要素可信流通带来挑战。因为数据要素易复制、易传播和难确权等特征，数据窃取、数据泄露等安全事件频发，为解决数据要素价值挖掘和风险防范之间存在的天然矛盾，实现数据要素的“可信流通”，成为学术界、产业界和政府组织关注的热点问题。

1.2.1 政府组织

近年来，国内外数据要素流通使用领域涌现大量意见和战略（如图 1），在国内，2022 年 12 月，中共中央、国务院印发的《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”）中，多次强调要促进数据可信流通。例如，在基本原则部分提出“建立数据可信流通体系，增强数据的可用、可信、可流通、可追溯水平”。在建立流通和交易制度部分提出“有序发展数据跨境流通和交易，建立数据来源可确认、使用范围可界定、流通过程可追溯、安全风险可防范的数据可信流通体系”，2023 年，围绕“数据二十条”各地各部门纷纷出台了数据要素流通交易的相关细则，例如北京市委政府印发了《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》的通知（以下简称《意见》），《意见》中提出了关于加强分类分级、数据安全和治理、数据监管模式创新等一系列措施和政策，被称为北京版“数据二十条”。2023 年 2 月中共中央 国务院印发《数字中国建设整体布局规划》，明确了强化数字中国的关键能力，包括构筑自立自强的数字技术创新体系和筑牢可信可控的数字安全屏障两大方面。随之在 2023 年 3 月，中共中央、国务院印发了《党和国家机构改革方案》，提出组建国家数据局。在 2023 年 10 月，国家数据局正式揭牌，国家数据局的成立有助于规范数据要素市场交易；有助于加强数据安全和隐私保护，降低数据滥用、数据泄露的风险，从近年来有关数据要素国家政策和法律法规的颁布，可以看出“国家安全”仍是数字中国发展的主线。

在国际上，2018 年 5 月欧盟正式推出《通用数据保护条例》（GDPR）用于保护欧盟公民个人数据。2018 年德国成立国际数据空间协会（IDSA）[1]致力于建立一个开放、安全、可信赖的数据生态系统，目前 IDSA 在全球范围内拥有来自 28 个国家和地区的 140 多个会员单位。2019 年德国和法国又相继联合推出基于身份识别和可信认证的数据基础设施信任平台：GAIA—X 项目。2019 年日本首次提出“基于信任的数据自由流动体系”（DFFT），提倡在保护个人隐私的基础上，打造安全、共享、互信的数据自由流动空间，试图打造美欧日数字流通圈。

英国在 2021 年和新加坡启动了数字贸易协议的谈判，致力于促进数据要素自由和可信的跨境数据流动。同年日本发布了《综合数据战略》，以“可用、可控、可信、互联”与“共创价值”为指导方针挖掘数据价值。2022 年 4 月欧洲议会通过了《数据治理法》希望可以通过可信的数据中介机构打破信任壁垒，促进欧

[1] 国际数据空间协会官方网站 https://internationaldataspaces.org/

洲数据高效流通共享。不同于欧盟宏观数字战略的制度导向模式，美国则是选择市场导向模式，在美国的数据交易流程中，主要是通过数据经纪人（Data Broker）作为可信第三方，构建一种“信用许可”体系进行数据交易。如同电商平台，当交易双方不具备可交易的信赖关系时，数据经纪人作为可信第三方，为双边履约提供了“担保”，从而纾解了双边数据交易的信任困境问题。

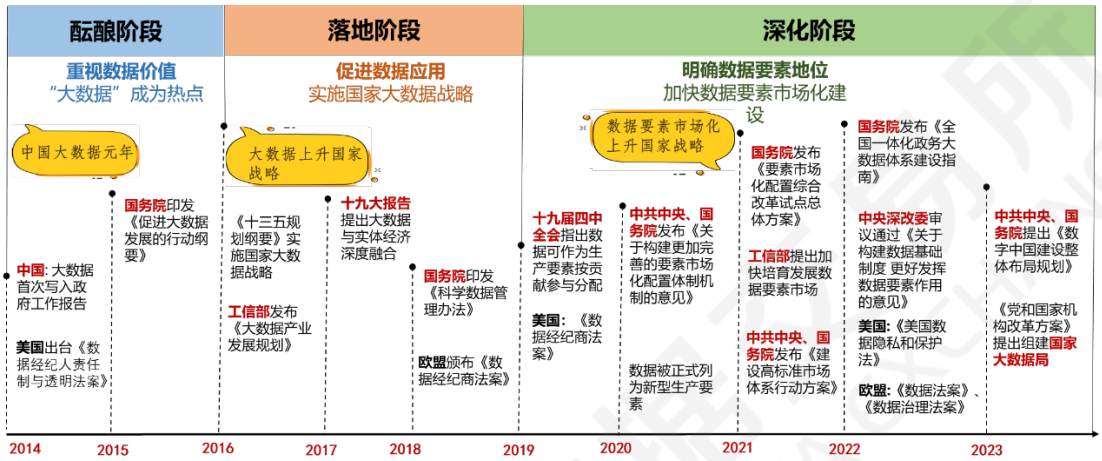

图 1 关于数据的政策布局

1.2.2 产业界

产业界也正在积极从技术支撑和规范管理入手，探索数据要素的可信流通交易范式，帮助数据要素市场建立可信生态。在可信环境技术研究上，北京国际大数据交易所结合隐私计算、区块链及智能合约技术、数据确权标识技术、测试沙盒等技术构建数据交易系统，为数据供需双方提供可信的数据融合计算环境。华为和中信银行为促进金融数据的可信流通提出了由数据可信流通管控中心、具有安全可信执行环境的可信数据空间连接器、安全存储资源池、以及安全的数据流通网络构成的金融数据可信流通解决方案[2]。在数据可信计算研究上，华控清交[3]推出了 PrivPy 多方安全计算平台，允许多个数据所有者在互不信任的情况下进行协同计算，输出计算结果。蚂蚁集团基于多方安全计算、联邦学习、可信执行环境、区块链等技术构建了蚂蚁链摩斯隐私计算平台[4]，通过计算前分级授权、计算中算法+规则双重保护，计算后日志审计，解决了数据流通使用过程中的数据安全和隐私保护问题。在数据可信学习技术研究上，腾讯基于联邦学习框架推出了“腾讯神盾沙箱”，能够让联邦学习各参与方在不披露底层数据和底层数据加密（混淆）形态的前提下，通过交换加密的机器学习中间结果，保证数据不出本地即可完成联合建模，最大化各个合作企业的数据价值。BaseBit.ai 自主研发了联邦学习框架 XFL[5]，XFL 不仅运用多种加密计算技术保护用户的原始数据不泄露，还使用了安全通信协议保护通信安全，实现人工智能模型的安全开发。在数据可信交付研究技术上，中国信息通信研究院则提出根据合约需求构建可信数据空间的框架，面向数据流通协议确认、履行和维护，解决多方

[2] 金融数据可信流通技术白皮书，中信银行和华为技术有限公司.
[3] https://www.tsingj.com/
[4] https://antdigital.com/products/morse
[5] https://www.basebit.me/sys-nd/21.html

主体之间的信任问题。上海数据交易所面向数据要素流通的全过程，研究构建数据可信交付框架，以构建内生安全的数据交易可信平台。

数据要素流通中的风险更多的来自参与者的机会主义行为，因此仅依靠可信流通技术还不足以保障数据要素市场的长期稳定，还需要管理规定来规范交易流程。在 2021 年上海数据交易所发布了数据交易配套制度，并确立了“不合规不挂牌，无场景不交易”的基本原则。北京国际大数据交易所也相继发布了《北京数据交易服务指南》，并积极探索建立监管沙盒、市场风险防控、交易规则等政策体系。贵阳大数据交易所在 2022 年发布了包括《数据交易安全评估指南》在内的数据交易规则体系，主要从交易主体登记、交易标的上架、交易场所运营、交易流程实施和监督管理保障五个方面进行了规定，以规范数据交易市场秩序。

截止目前数据交易机构已有 60 家，随着各地数据交易机构在科学技术上的研发和管理制度上的创新，数据要素市场正在向诚信、互信和可信的数据交易生态有序发展，如图 2 所示。

图 2 数据要素市场生态

1.2.3 学术界

数据要素可信流通也在学术界引起广泛关注，在市场制度建设方面，文献[10]从政府层面研究了政府数据资产管理的要素框架和运行模式，提出可信数据生态，但缺乏对企业数据、个人数据可信管理的探讨。文献[11]基于场内交易视角，从制度层面构建数据事前可信交易体系，重点关注交易前的合规审查与合法性确认，交易过程透明等问题。黄京磊等人[12]提出一种新型可信的数据流转模式—数据信托，通过设计数据信托运行机制和相关制度，提出数据信托的组织结构、特征、功能和监管方案等，有效隔离参与者的市场风险，从而增进数据要素市场的可信性。包晓丽和杜万里[13]从场内交易视角，构建数据要素可信流通制度体系，重点回答数据进场交易的功能意义、交易前的合规审查与合法性确认、交易过程的公示公信等问题。林镇阳等人[14]提出从“数据要素、数据业务主体和制度规范”三个维度，构建包括“数据流—业务流—信任流”在内的价值驱动的可信数据要素市场化生态系统，并从生态系统视角构建数据运营平台的监管体系，动态持续监管整个数据生命周期，保障数据进行长期保存、组织、维护、利用等。在业务管理制度层面，相关研究主要围绕数据流通使用的业务环节制度设计展开。例如在交易申请环节，范文仲[15]指出，一个合规可信的交易模式，需要实现“上市有审核、采买有资质”，建立数据源的合法性审核制度和售后管理制度等。在交易磋商环节，Rohn 等人[16]提出，数据交易平台不仅要构建资产交易的撮合、交割和清算机制，还要能够为数据供方和数据需方

创造价值并实现价值交付或分配。在交易实施环节，很多研究者提出通过安全计算技术实现数据的流通交易和价值释放。窦悦等人[17]指出不同的隐私计算平台的算法原理和系统设计不一致，使得异构平台间难以进行信息的交互，容易形成数据壁垒，如何构建异构隐私计算平台间的互联互通方案亟待进一步的研究。在交易结束环节，安全审计作为一种监督手段，有效迎合了数据要素市场合规可信的管控需求，面对数据要素流通安全风险的复杂性，需要建立一套成熟的交易安全审计策略[18]。

在数据要素可信流通的影响因素研究方面，文献[19]面向主体可信进行了讨论，认为不同主体在交易中扮演的角色、市场能力、交易行为以及他们之间的相互作用是影响数据要素可信流通使用的关键因素，但缺乏对市场其他要素可信的探讨，如数据可信。文献[20]认为不可信数据带来的风险会在数据价值链中所有关键环节传播，强调了数据可信的重要性，但是缺乏对数据可信属性的进一步研究。

综上所述，虽然学术界围绕数据要素流通使用的可信问题，在管理制度、技术体系等方面已经开展了大量研究，取得了丰富的研究成果。但现有对管理制度与支撑技术的研究是两条独立的研究路径，也多是从主体可信或数据可信单方面讨论数据要素的可信流通问题，缺乏对数据要素可信流通使用整体的刻画。

数据要素流通与其他传统商品流通具有显著差异，且数据要素流通使用过程涉及参与主体多元、数据类型多样、交易合约复杂、使用算法多变等特点，有关不同类型可信因素间的相互联系，以及不可信因素对数据要素可信流通使用的作用机制需要开展深入研究，以建立数据要素流通使用的可信模型，揭示数据要素流通使用的可信机制。

二、数据要素流通交易中的信任理论及概念

2.1 信任的本质及相关理论

2.1.1 信任的本质

数据要素市场一直以来存在双向信息不对称问题，即在数据交易前买方无法掌握数据质量、数据来源等信息，相比数据卖方，买方处于信息劣势地位。在数据交易中后期，数据卖方则无法得知买方的数据使用行为、是否转卖等信息，此时卖方处于信息劣势地位。数据要素市场的双向信息不对称会带来道德风险、数据泄露风险等问题，影响数据安全、人民隐私安全，甚至国家总体安全，这些问题在现实中往往表现为信任问题。

信任作为行为学、心理学、管理学和经济学等多个领域共同关注的话题，学者们也从多个角度给出了信任的不同定义。心理学家从认知、情感、经历和人格特征等因素出发，认为信任是一种期待心理或预期行为的个人化反应[21]。经济学家则是将信任看作个体在风险与收益之间博弈的一种理性选择[22]。在行为学领域普遍认为信任是基于对对方表现出行为的预期，而愿意处于受对方行动影响的薄弱状态[23]。而在管理学领域中更多的是用参与、控制、制度及合约等内容去建构信任的涵义[24]。Rousseau 等人[25]整合了不同学科的观点，将信任定义为一种自愿将自己放在易被伤害地位的心理状态，这种状态是基于个体对他人意图和行为的一种积极期望。在数据要素流通交易情境下，即期望被信方的交易意图和交易行为不会损害信任方的利益。

2.1.2 信任理论

随着信任理论的不断发展，学者们将信任根据不同的标准将信任划分成多种类型。我们对信任理论进行了简要的梳理，并识别出数据要素流通交易中的信任应当包括哪几种类型。Zucker 根据信任的来源不同，将信任分为三类：经验信任、特征信任和制度信任[26]。经验信任是主体根据以往交易历史，对市场其他主体有初步的了解，从而建立起来的信任关系。特征信任是指个体之间的信任建立在对对方具备特定特征或属性的信念之上，这种信任也可以是来源于群体规范，因为规范对成员行为的约束作用，从而不同的群体在市场上具有不同的可信度。制度信任则是在给定制度下，主体迫于制度惩罚带来的违约成本，不得不采取守信的决策行为。在社会学领域，Luhmann 的社会系统理论将信任分为人际信任与系统信任，人际信任则表示信任个体与被信个体之间的信任关系，而系统信任则是主体对群体、机构、市场或者是制度的信任，Luhmann 认为系统信任取代人际信任是市场不断发展的必然结果[27]。Sako[28]研究了在买卖活动过程中的信任关系，提出了合同信任、能力信任和声誉信任。合同信任来源于对另一方道德水准的依赖，相信对方会信守既定的协议，无论是这个协议是口头协议还是书面协议；能力信任是指一个人在对他人或者某个系统的信任中，主要基于对其能力和技能的评估和信赖，能力信任建立在认为对方具备足够的知识、经验、技能和资源来完成某个任务或者达成某个目标的基础上。声誉信任是指在与他人互动时，基于对其良好意图和善良行为的信任和依赖，这种信任是建立在我们认为对方有良好动机和诚实行为的基础上。

2.2 数据要素流通交易过程中信任关系的形成机制

信任在数据要素流通交易中起着重要的作用，普遍认为，信任可以降低数据评估成本、简化交易流程，是数据要素市场得以良好运行的润滑剂，但是数据交易的盲目信任不仅会给企业带来经济损失，严重的还会危害国家安全。虽然信任在各个学科中已经得到了充分的研究，但对数据要素流通交易框架下的信任问题还缺乏系统性的探讨。本报告将通过对已有的信任理论与数据要素市场的信任困境相结合，阐述数据要素可信流通交易过程中信任关系的形成机制。

Zucker[26]认为信任来源于：经验、特征和制度。数据要素市场的经验信任来源于过去双方的交流和交易，由经验建立起来的信任关系往往是有限的，尤其对于首次参与数据交易的主体。特征信任则是在对方客观事实基础上的一种主观认知，在数据要素市场，不同类型主体的可信任特征有所不同，例如数据需方可能基于以下几方面对数据供方的可信任特征做出评价：数据供方的资质条件、数据处理水平、沟通服务能力等，但是数据供方可能是基于另外几个方面对数据需方的可信任特征做出评价：数据保护能力、行为可靠性、合同的履行等。其中由于制度产生的信任来源于对公开透明、有公信力的社会规章制度的信赖，如资质证书、信用证明和各种法律法规的保证产生的信任。Sztompka[29]认为信任的重要基础是强制性的监督和惩罚机制。但我国包括数据产权制度、数据要素流通和交易制度、数据要素收益分配制度等内容在内的数据基础制度体系还有待建设。

Sako[28]则从企业采购与销售活动中的信任关系出发，提出了三种新的信任来源：合同信任、能力信任和信誉信任。在数据要素流通使用中充满数据滥用、数据泄露和攻击等诸多风险的情况下，签订合约是预防双方机会主义行为的有力手段。因为合约可以起到约束行为的作用，可以降低主体数据交易的不确定性，提高交易的可信任水平。但是由于风险的不可预测性，交易双方无法通过合同对所有风险做出详尽的约定。进而提出了能力信任，一般会通过观察或企业履约能力测评认证证书获取对方履约能力和技能的信息，以建立能力信任关系。在数据要素流通交易的场景中，数据供方普遍会关注数据需方是否具有良好的数据保护能力以应对外部攻击风险，而数据需方可能会更加关注供方的数据采集、数据处理等能力以降低数据质量风险。声誉信任来源于对方履约动机的评估，是一种相信对方会履行约定、不会侵犯和泄露隐私的善意信任。声誉可以分为基于过去双方长期交往或交易的直接声誉和基于信用评价和信息传递的间接声誉，Bohnet 和 Huck[30]通过实证研究发现这两种声誉都对市场的信任水平和可信水平产生积极影响。数据要素市场作为一个双向信息不对称的市场，声誉机制的引入（如资质评估、交易评价等）可以有有效缓解市场中的道德风险问题。

Lucy[31]从博弈的角度提出了策略信任。策略信任主要指数据供方只有在需方通过数据交易产生的价值大于违约带来的风险收益，或者交易违约成本大于数据滥用、转卖的收益时，才会选择建立信任关系，是一种通过理性博弈后形成的信任。

从上述对数据要素市场中信任关系的分析，建立数据要素可信流通交易机制不仅需要明确的惩罚机制以约束不可信的行为，还需要建立信用体系提高整个市场的可信水平，使诚实、守信和公平交易成为数据要素市场参与主体的行为准则。

三、数据要素流通交易中的可信风险识别

数据要素流通使用环境复杂，参与主体类型多、交易过程环节多。如何有效识别数据要素流通使用中存在的可信风险？本报告从主体（业务生命周期）、客体（数据生命周期）和环境（流通使用技术）视角，对可信风险进行了系统识别。

3.1 业务生命周期视角的主体可信风险分析

业务生命周期指数据要素流通使用的全过程，本报告根据文献[32]将数据要素业务生命周期划分为交易申请、交易磋商、交易实施和交易结束四个阶段。

交易申请阶段的安全风险可归纳为交易主体资质安全风险、数据准入安全风险和产品质量风险。数据要素流通使用过程涉及供方、需方、交易服务机构等多方主体，主体资质直接关系到数据来源和流通使用的合法合规性[33]，肖建华等人认为不同交易主体应有不同的资质审核要求，对于法人主体，交易平台需要审核其法人信息、营业执照、税务信息等；对于个人主体，交易平台需要审核其身份信息、交易目的、数据使用范围等[34]，确保数据交易参与主体不存在法律、法规禁止或限制的任何情形；数据是流通与使用的标的物，如果出现不合规的数据流入市场有可能严重影响个人隐私安全、商业安全和国家安全，数据准入安全风险需重点关注数据产品是否包括禁止交易数据、未授权的个人数据、商业机密数据等；参与流通使用的数据要素除需满足准入的安全要求外，还要考虑数据质量风险。若因审核不严而使伪造或错误的数据上线，可能导致基于数据的分析结果无效，给需方造成巨大损失。

交易磋商阶段主要存在供需匹配风险、交易公平风险和交易透明风险。在供需匹配上，数据市场中充斥着大量的数据，面对丰富的、不同规模、不同重点的数据供给，如何找到最适合需求的数据非常困难，匹配在时间和质量上能否契合成为供需匹配的最大风险；在交易公平性上，由于大多数的数据流通使用通过既充当交易的组织者又充当裁判的数据交易平台进行，如果出现平台与买方或卖方合谋，交易的公平性将难以保证，此外，由于数据产品边际成本接近于 0，使得卖家具备了实施价格歧视的更大弹性；在交易透明性上，供方往往面临着数据如何出售、哪些数据更有价值的挑战，需方无法获得数据的透明访问，了解原始数据的真实性；供需双方在支付细节、上市、数据发现和存储等方面缺乏透明度保证。

交易实施阶段的安全风险主要体现在权限分配、定价和交易清结算方面。在数据交易中，交易的不仅是数据本身，更是与之相关的各项权限，数据产品交割后所有参与者主张的排他性权限能否得到保障，关系到数据要素流通交易能否顺利进行。数据作为一类特殊产品，相较于传统商品，在成本上以及消费单位、聚合性、消费方式、再利用和转售上存在着巨大的差异，导致了在定价原则和方法上的不同考虑，版本控制成为设计和定价数据要素的常用机制，不同版本的价格可以与不同客户群体的价值相关联。这对数据要素的定价提出了一系列新要求，其中包括公平性[35]、无套利[36]、真实性[37]、隐私保护[38]以及计算效率[39]等要求；与此同时，数据要素定价还面临着与传统市场类似的操纵风险，即恶意打压或哄抬价格等。在交易清结算时，供需双方均可能面临交易违约风险，需方付款后所收到数据的真实性、时效性和完整性是否与供方声称的一致，供方是否会因为需方发生拒不交付、抵赖等行为导致其无法得到约定的款项。

交易结束阶段违规使用、转卖、再识别等安全风险。在交易结束阶段，安全风险主要来自于需求方。当数据交付给需方后，面临着不诚实的数据需方没有按照约定而是超范围地使用数据，从而侵犯供方的合法权

益，甚至威胁多方安全，面临着需方将其购买的数据产品进行二次流转、转卖的风险。尽管在数据交易前，已对涉及用户身份信息的数据进行清洗、加密、匿名化等操作，但是随着公开资料的不断增多和互联网信息技术的不断发展，经过匿名化处理的数据都有可能被再识别。

3.2 数据生命周期视角的客体可信风险分析

数据生命周期指数据从产生或获取到销毁的全过程。本文按照数据要素流通使用的相关操作流程，将数据生命周期划分为采集存储、交付传输、加工使用、备份销毁四个阶段。

采集存储的安全风险主要有采集安全风险、侵权风险和存储安全风险。数据采集的质量标准会影响整个链路的数据质量，原始数据的真实性、完整性、可靠性直接关系着后续的数据挖掘和分析工作[40]；如果采集的原始数据无法反映客观真实的情况，在此基础上的模型预测结果就会出现偏差，影响数据产品的可用性[41]。数据采集时还需要严格遵守用户知情同意和最小必要等相关法律原则，但在实际中不少智能设备厂商和 app 公司为了精准营销，得到更准确的用户画像，而过度收集用户个人信息，甚至“监听”用户的智能设备，使用户在网络空间中变为透明人，严重侵犯了个人知情权、隐私权等。数据一般存储在云端或分布式文件系统中，云端直接加密会带来巨大计算开销，增加密钥管理风险，而分布式存储中一个节点或多个节点遭受攻击，可能直接影响计算结果。

交付传输的安全风险主要源自网络硬件风险和外部攻击风险。数据在长距离网络传输过程中，面临着网络不稳定导致的数据包丢失风险、网络带宽不足导致的传输时效风险，特别是面临大规模数据传输时网络硬件风险将更加突出；数据在多路径中快速集群和转发，容易遭受病毒植入和攻击，大规模数据的汇集与传输会降低外部攻击成本，提高单次攻击的收益，从而引起黑客的攻击，用户与服务器间共享和生成密钥是数据传输中的重要风险点，社会工程已经成为外部攻击和窃取数据的一种重要手段。

加工使用的安全风险突出表现在隐私泄露风险、安全攻击风险和数据滥用风险。从原始数据得到可流通交易的脱敏数据、模型化数据，必须借助大数据技术进行脱敏、分析、测试等加工操作[39]，但大数据技术在学习训练过程中面临着两类隐私泄露风险，即非授权用户直接获取数据的隐私泄露风险和攻击者通过一定方式推断数据集中敏感信息的隐私泄露风险。在数据加工使用时，还容易遭受来自多方面的攻击，如伪造数据或修改数据、攻击模型参数、恶意攻击服务器等。由于数据要素的使用用途和用量难以监控和衡量，受利益驱动，在数据使用过程中往往存在超权限使用现象，甚至滋生出非法数据交易产业链，对个人隐私、国家安全造成严重危害。

备份销毁的安全风险有备份审计安全风险和销毁安全风险。数据流通交易结束后需要生成相关交易日志并进行备份，但备份过程可能存在未经授权擅自更改或删除、异机备份等情况，无法为交易过程的查询、分析、审计和争议仲裁等提供可靠依据。数据销毁安全是指在监管业务和服务所涉及的系统及设备中清除数据时，通过建立针对数据的删除、销毁、净化机制，防止数据被恢复而采取的一系列防控措施。不及时、不彻底的销毁给内部人员和黑客提供可乘之机，可能产生数据泄露、个人信息重新识别、数据二次转售等恶性影响，特别是当数据存储在云端时，云服务商可能拒绝按照用户的删除指令销毁数据，而是恶意保留数据，从而使其面临被泄露的风险。

3.3 流通使用环境视角的环境可信风险分析

流通使用环境是指数据要素在流通使用的整个业务生命周期中所涉及的环境。具体而言，可分为流通交易平台、软件环境、硬件环境三大部分。数据要素流通使用过程中，从交易申请到交易结束的全过程都在流通交易平台中完成，检测、脱敏、挖掘等各个具体操作都依赖于流通交易平台的大环境实现；同时，数据要素的汇集整理、建模分析等计算操作是依靠软件环境的相关算法实现的；而软件中算法的运行需要硬件基础设施提供算力资源才能完成。

流通交易平台的安全风险主要表现在访问控制能力、环境应变能力、运行能力和内容交换控制能力。访问控制能力是指有益用户都应能访问系统，而有害用户都应被拒绝，体现了平台的可扩展性和安全性；环境应变能力是指平台对内外部变化应具有的灵活性和可靠性，一方面体现了平台可以在不同的环境下运行，另一方面体现了平台内部结构的相对稳定性；运行能力是指平台有效实现数据要素流通利用的性能，有用性体现了平台的事务处理能力，易用性是指实现业务功能时占用最小系统资源的能力从而保证系统的运行性能，如访问速度快、操作方便等；内容交换控制能力是指平台的连通性和隐私性，要求既能够保障正常内容的交换，又能保护隐私内容。

软件环境的安全风险体现在系统软件风险和应用软件风险。数据要素流通使用过程中需要各类系统软件和应用软件的支撑，这些软件存在着各种各样的漏洞甚至隐含着恶意代码，而检测此类软件中存在的恶意代码非常困难，给数据要素流通使用带来了巨大的潜在风险。算法是数据要素流通应用中的一类特殊应用程序，随着各类深度学习模型、协同学习模型的应用，算法的计算逻辑、交互逻辑日益复杂和多样化，使得算法结果的可解释性差强人意，算法自身的安全性也难以控制，此外很多算法的设计基于某种安全假设，例如，假设多个参与方之间均遵守指定规则及协议流程且不存在同谋等，这额外地增加了一种安全假设风险，即当算法的安全假设不能被满足时，算法结果可能会难以预料[6]。

硬件环境安全风险指数据存储、运行等所需要的关键信息基础设施安全风险，主要分为计算机物理安全和计算机网络安全。计算机物理安全风险包括计算机的异常损毁、被盗、非法使用等；计算机网络安全风险包括对计算机网络设备、计算机网络系统、数据库等的攻击行为。此外，供应和搭建硬件环境的厂商是否可信任、是否曾发生未经允许自动读取设备信息和产品质量不合格事件、设备是否存在故障、传输是否存在延迟、是否存在硬件木马等都是与硬件环境相关的安全风险。如果硬件设备易遭受攻击、频频出现故障，将严重影响数据要素相关产业的健康发展。

[6] 云程发轫，精耕致远 中国隐私计算行业研究报告[C]//.艾瑞咨询系列研究报告（2022 年第 3 期），2022:1026-1110.

四、基于 PDCA 的数据要素可信流通交易评估指标和测度体系

4.1 “PDCA”信任模型

本报告依据数据要素流通交易全流程可信的要求，即事前审查阶段需要保障主体资质可信、数据质量可信和合约内容可信，在事中监控阶段要保障主体行为和算法行为可信，在事后审计阶段，要对数据流通使用过程进行追溯，更新主体和数据的信用评估。本报告面向数据要素流通交易过程涉及道德关键主体和客体，提出了 PDCA 可信模型，即主体可信（Participant）、数据可信（Data）、合约可信（Contract）和算法可信（Algorithm）。（如图 3 所示）

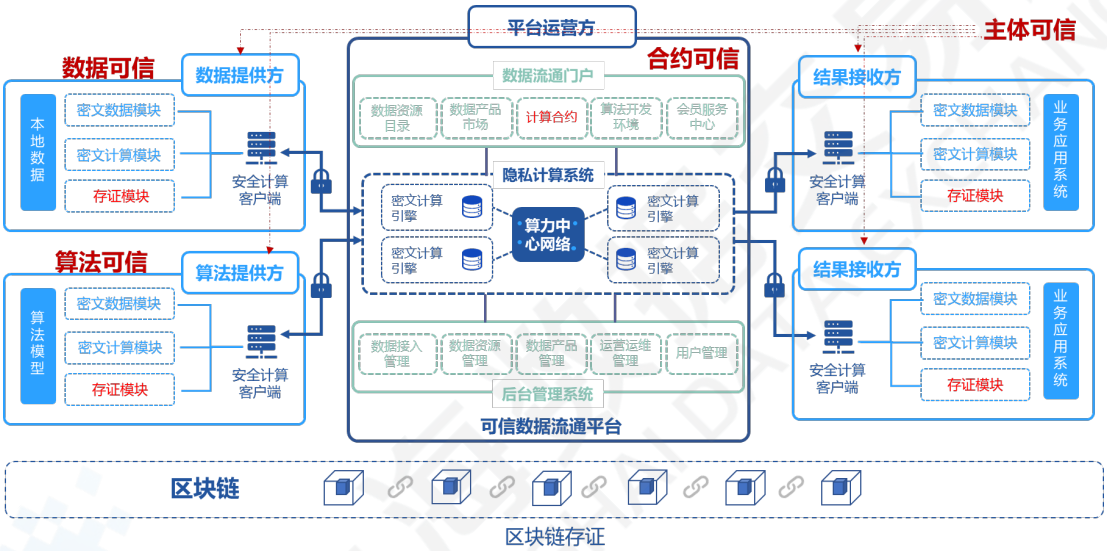

图 3 数据要素可信流通使用体系

（1）主体可信

主体是数据要素市场运行的引擎，包含了个人、企业和政府等多元主体，各主体之间的信任关系和相互合作构成了数据要素可信流通的底层逻辑。不同主体在交易中扮演的角色、市场能力、交易行为以及他们之间的相互作用是影响数据要素可信流通使用的关键因素。不可信主体可能会造成数据要素市场的瘫痪，加大市场的数据质量风险、交易道德风险和违约风险。例如，由于数据要素具有易复制性的特点，不可信的数据供方可能会转售他人数据，侵害数据实际拥有者的合法权益；而不可信数据需方可能滥用数据，包括未经授权的数据访问、数据滥用、数据泄露等行为。因此，拥有数据的企业出于对其他主体道德风险的感知，为维护自身的利益，往往不愿意甚至不敢将数据出售给其他企业，极大阻碍了数据要素价值的释放。

此外，由于数据要素在流通使用过程中数据供方无法得知自己的数据将被如何使用以及数据需方是否具有数据保护的能力，数据需方也很难向第三方证实自己是否滥用了供方数据。这种信息不对称性和不可证实性造成了主体间的信任壁垒问题。因此，保障主体可信可以降低主体间信任沟通的成本，提高数据要素流通的效率。

（2）数据可信

数据是数据要素市场发展的血液。可信的数据供给可以促进数据跨区域、跨行业配置，降低企业的数据获取和科技创新的边际成本，提升数字经济产业链供应链的质量。数据是数据驱动分析和预测的基础，低质量的数据可能会导致错误的业务判断和预测，损害企业的利益，可能造成“劣币驱逐良币”的现象。此外，不规范的数据可能存在数据泄露和安全威胁的风险，甚至危害国家总体安全。另一方面，由于数据要素具有易复制和可分割等特征，不合规数据带来的风险会在数据价值链中所有关键环节传播，例如数据产品化过程中的不合规风险会传播到数据服务、数据应用的开发过程中。此外，数据要素还具有确权难、难估值的特征，来源不真实的数据可能会损害数据拥有者的合法权益，从而损害数据要素市场可持续发展的动力。可信数据的流通可以提高数据利用效率、提升数据要素价值，扩大市场需求，实现数据要素市场发展的正向反馈。

（3）合约可信

合约是数据要素市场稳定的保障。虽然数据要素市场的交易机制具有多样性，但是供需双方签订合约可以就数据的使用量和使用方式、数据所有权和使用权及个性化数据服务等内容做出约定，规范数据交易流程，保障数据要素流通使用的可信可控。不可信的合约往往难以有效约束市场参与主体的交易行为，例如。因为数据要素市场存在反向信息不对称问题，在数据交易过程中是由买方占据信息优势，买方比卖方则是掌握更多关于数据用途、未来收益和风险程度等信息，此时卖家可能会减少出售数据，甚至不出售，进而导致从供给侧引起市场失灵，导致“有数无市，有市无数”的现象。由于数据具有非竞争性的特点，同一数据可以同时被其他主体使用，这意味着即使合约中规定了数据禁止转售、重复利用等条款，也无法完全让数据供方相信，因为数据需方一旦购买数据，就可以不依赖数据供方自由支配数据用途。可信的合约可以为数据交易合作的双方带来互惠和双赢，例如在合作初始阶段建立信任关系，降低双方的交易成本。根据关系契约理论，交易合约考虑的是双方在将来某个时刻进行某种行动所许下的承诺，由于无法预见数据使用过程的各种风险，再加上不能完全预测到签订合约时可以预见的全部信息，所以需要一份可信的交易合约使双方可以更好的应对数据泄露、数据滥用等各类风险。同时也增加了双方连续合作的可能，从而形成良性循环。

（4）算法可信

算法是数据要素价值释放的工具。任何学习算法没有绝对的安全，算法协议安全和算法性能优化是数据价值挖掘面临的两大挑战。例如，联邦学习虽然只需要较少的性能开销，但是在传递梯度信息过程中，可以根据梯度信息推测出原始数据，存在数据泄露的风险。因此，不可信的算法可能存在安全和隐私风险，对个人隐私造成威胁。其次，不可信的算法可能会带来算法公平性问题，由于训练数据或者特征选择的偏差，算法决策可能会存在歧视或偏见，例如在招聘、贷款审批等领域，因性别、种族等敏感属性特征产生不公平的结果。最后，不可信的算法即使耗费了大量的算力和数据资源，也有可能提供错误的数据处理结果，进而导致错误的决策。因此，算法可信可以更好的解决数据要素流通使用过程中隐私保护和价值挖掘之间的矛盾，让数字经济的安全和发展可以并驾齐驱。

4.2 评估指标体系

结合上述分析，本报告从构成数据要素可信流通使用的关键要素，即主体可信、数据可信、合约可信和算法可信 4 个方面来构建数据要素可信流通使用的评价指标体系。如图 4 所示。

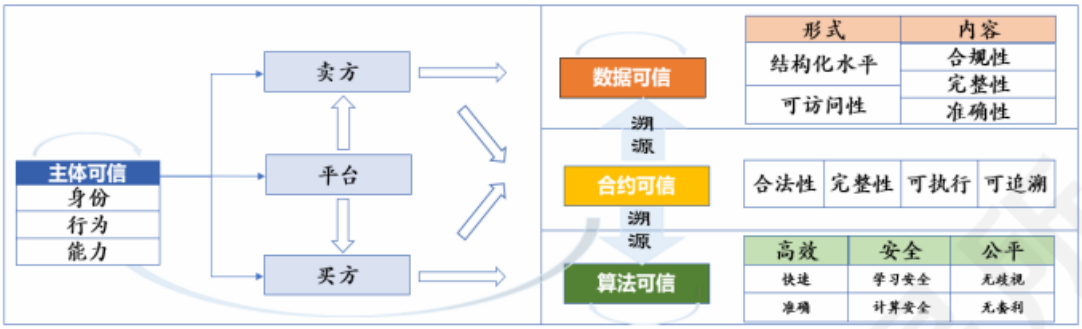

图 4 数据要素可信流通使用评估指标体系

(1) 主体可信指标的选取

主体可信（Trusted Participant，TP）是衡量数据要素流通使用过程中各类参与主体（数据供给方，数据需求方和第三方数据服务商等）的身份资质、交易行为、履约能力等各项指标的可信度，参与主体具备一定的可信度是参与场内数据供给、数据使用和数据服务的前提。国家标准《企业信用评价指标》GB/T 23794—2023 在履约意愿、履约能力和履约行为三个方面规定了企业信用的评估的基本指标，履约意愿指的是企业的价值理念与品牌形象等内容，主体的身份信息与标准规定的企业履约等内容息息相关。

依据国家标准，结合数据要素流通使用领域对可信主体的普适要求，可以将主体可信的指标分为三类：身份可信、行为可信和能力可信（如表 1 所示）。

表 1 主体可信评价指标

一级指标	二级指标	指标描述
主体可信（TP）	身份	主体资质的合法性、真实性、有效性。
	行为	流通使用历史行为中的合规合法水平，履约成功率、履约效率、履约质量等。
	能力	采集存储、交付传输、加工使用、备份销毁及数据保护等技术能力，健全的内部管理制度及作业流程。

(2) 数据可信指标的选取

数据可信（Trusted Data，TD）是指在数据要素市场流通使用的数据集在形式规范、内容完整、内容准确等各项指标的可信度，数据作为数据要素市场交易标的物，保障数据的真实可信是数据要素市场可持续发展的基础。从数据产品使用者角度来看，使用者更加关注数据量是否丰富、数据来源是否权威、数据准确性、数据一致性、数据时效性以及元数据信息等。从监管者的角度来看，监管者更加关注数据内容的合规性、可溯源性和明确的应用场景。数据可信的评估是一个多维度的概念，既有不因场景和消费者的差别影响评价的客观方面（如准确性、及时性），也有与使用数据的决策者的感知有关的情景方面（如相关性和可用性）。例如，对于图片数据更加关注对比度、清晰度、亮度等质量特征，对于文本数据可能更加关注准确性、完整性等质量特征。

基于先前的交易实践，对数据质量的要求可以分为内容要求和形式要求，因为本报告将内容可信和形式可信作为评价数据可信的二级指标（如表 2 所示）。

表 2 数据可信评价指标

一级指标	二级指标	指标描述
数据可信（TD）	内容	（1）合规性：数据来源真实程度、敏感数据去标识化程度。 （2）完整性：数据的属性、数据项、时空覆盖率等数据内容的完整程度。 （3）准确性：数据准确表示其所描述的真实实体的程度。
	形式	数据的属性覆盖率、数据项完整度、时空覆盖率等

(3) 合约可信指标的选取

合约可信（Trusted Contract）是指数据要素市场参与主体之间建立的契约或合同的合法性、完整性等指标的可信度，确保合约可信可以有效约束市场主体的交易行为，减少违法违规数据交易事件的发生，促进数据要素市场健康发展。合约作为一种完全契约机制，基础要求是就双方的权力和义务做出约定。合约一个明确的、可约束的、保证实施的约定，内容包括明确合理的监督与奖惩机制，即合约要保证完整性，除此之外，合约作为具有法律约束力的两方或多方之间的书面协议，需要保证内容的合法性。现有的合同治理策略是从合同条款的明确性、适应性和履行的严格性三个维度进行评估。合约是否被严格履行与可约的可追溯性密切相关，合约的适应性也反映了合约的可执行性。基于此，本报告从合约的合法性、完整性、可执行性和可追溯性 4 个指标作为合约可信的评价指标。（如表 3 所示）

表 3 合约可信评价指标

一级指标	二级指标	指标描述
合约可信（TC）	合法性	合同是否具有法律约束力，是否符合相关法律法规的要求。
	完整性	明确界定了合约双方的责任、权利、义务，特别是数据交付、使用范围以及隐私条款和保护措施。
	可执行性	是否考虑了价值约束、风险约束和成本约束。
	可追溯性	可以跟踪合约履行过程并能进行有效核验。

(4) 算法可信指标的选取

算法可信（Trusted Algorithm）从算法价值的角度，算法的应用应该促进数据流通和使用，带来技术上的变革和管理效率上的提升。同时从算法伦理的角度，算法应该在社会伦理的约束下被开发以及被使用。在学术界和商界已经有了很多关于可信 AI、可信模型的讨论，有学者提出了公平性、隐私性、可解释性、可问责性和可接受性 5 项可信 AI 的要求，也有学者从算法的可解释性、公平性和透明性等指标讨论了用户对互联网平台算法的信任。本报告从法律方面的合规信任、技术使用方面的功能信任和社会价值方面的伦理信任定义了算法可信。合规信任包括安全可靠、过程可控、责任明确等影响因素；功能信任包括功能适用、性能效率、准确稳健等影响因素；伦理信任包括公平性、可解释性和鲁棒性等影响因素。基于此，本报告选取了代表算法合规信任的安全性、算法功能信任的高效性和伦理信任的公平性作为算法可信的评价指标，如表 4 所示。

表 4 算法可信评价指标

一级指标	二级指标	指标描述
算法可信（TA）	高效	算法执行过程中的资源占用、计算效率、计算结果的准确性等。
	安全	算法输入鲁棒性及抗攻击鲁棒性。
	公平	算法决策的无偏向性、无套利性、可解释性。

4.3 指标测度体系

客观全面的评价是建立数据要素可信流通体系的关键，为构建数据要素可信流通体系，应设计相应的可信度量方法。本文从国家政策制度、国家标准和国内外文献获取到数据要素可信流通使用的关键指标测度方法，如表 5 所示。

表 5 数据要素可信流通使用的关键指标测度方法

一级指标	二级指标	审查对象	测度方法
主体可信	身份（TP1）	注册登记、营业执照、资质证书、有无违法记录等	人工查验
	行为（TP2）	履约效率、数据服务质量、数据交易客户评价等	主题分析
	能力（TP3）	专利、技术报告、年度报告等涉及到的数据保护技术、数据处理技术等	主题分析
数据可信	内容（TD1）	数据来源、敏感数据、数据实体、数据域、数据引用和数据定义等	基于学习的数据评估
	形式（TD2）	数据项命名、数据格式、数据类型、数据长度和数据结构等	基于规则的数据评估
合约可信	合法性（TC1）	合约条款是否符合数据出境安全、人民信息保护安全等	法律知识图谱
	完整性（TC2）	数据内容、数据用途、交付质量、交付方式和参与方安全责任、保密条款	合同信息抽取技术
	可执行性（TC3）	经济价值范围、风险的分担和责任的规定、成本的限制等	合同信息抽取技术
	可追溯性（TC4）	关键追溯点（CTPs）	关键追溯点的数量
算法可信	高效（TA1）	准确性、精确度、召回率、F1 评分、时间复杂度和空间复杂度等	算法执行时间、CPU GPU 占用率、准确度等
	安全（TA2）	异常输入、数据偏差、噪声容忍度、对抗攻击等	鲁棒性测试方法
	公平（TA3）	算法预测或分类的结果在不同群体中的差异	差异影响、人口均等、机会均等、个体公平等

(1) 主体可信指标测度

对于主体的身份可信，可以根据国家标准《信息安全技术-数据交易服务安全要求》对数据供需方和平台的要求，对主体的资质进行一一查验，例如一年内无重大数据类违法违规记录的合法组织机构，以及具备相应的数据安全保障能力等内容，但是标准中并未指出主体数据保护能力的测度方法。对于行为可信和能力可信可以采用基于动态主题模型方法，将主体的所有历史交易评价数据看作一个文档，通过动态主题模型训练得出服务态度、履约效率和数据质量等文档主题的分布，根据主题出现的概率测度主体的行为可信。同理，可对主体的专利、技术报告、年度报告等文档进行主题分析得到主体的管理能力、数据保护能力等相关主题的概率分布，使用不同能力主题的概率分布测度主体能力可信水平。

(2) 数据可信指标测度

数据内容可信测度，依据数据内容与数据交易标准规范的契合度评估数据的合规性，可以考虑采用区块链溯源技术度量数据来源的真实程度，还可以使用敏感数据识别技术检测敏感数据去标识化的程度。在数据完整性上，从数据的属性覆盖率、一致性、可获取性等维度测度数据内容的完整性。国家标准《数据质量 第 8 部分：信息和数据质量：概念和测量》从数据的实体、引用、域和用户定义的完整性四个维度度量。在数据形式的可信指标测度方面，可以从数据项命名、数据格式、数据类型、数据长度和数据结构是否符合既定规范来度量数据的语用质量。

(3) 合约可信指标测度

在合约合法性测度方面，应依据《数据安全法》、《网络安全法》和《个人信息保护法》等法律法规，审查合约内容是否符合数据出境安全、人民信息保护安全等要求。在合约完整性测度方面，需要根据国家标准《信息安全技术-数据交易服务安全要求》审查主体之间签订的三方合同是否涵盖了数据内容、数据用途、交付质量、交付方式和参与方安全责任、保密条款等内容。使用人工一一审查合约条款的合法性，不仅效率低下，还增大了合约评估的成本，可以考虑采用法律知识图谱审查合同的相关条约，对合约条款给予合法性测度。因此，在智能合约撮合过程中，推荐算法成本约束、价值约束和风险约束的权重占比可以用来测度合约的可执行性。合同的可追溯性指的是能够准确地追溯和回溯合同的履行过程和相关事项，可根据合约中规定的关键追溯点（CTPs）的数量来测度合约的可追溯性。

(4) 算法可信指标测度

算法的高效性即包括算法的性能评估，还包括资源的占用情况。常见的性能测度包括准确性（Accuracy）、精确度（Precision）、召回率（Recall）和 F1 评分，在资源占用方面常见的测度包括算法的时间复杂度和空间复杂度。在算法安全性方面，Katzir 等人[42]提出了一种模型鲁棒性评分测度方法，该方法是通过量化应用于网络安全的各种机器学习分类器的弹性来评估算法的鲁棒性。还可以通过设计测试用例的方法测度算法的输入鲁棒性，如异常输入测试、噪声容忍度测试、数据偏差测试等。

文献[43]介绍了在预测任务中算法公平性的测度：差异影响（disparate impact），该测度表示阳性预测的比例在不同群体中应该是相似的，如果一个阳性的预测结果表示贷款批准，那么被批准的贷款人的比例在不同的群体中应该是相似的。差异影响测度的计算方式见式（1）。

$$\frac{P\left[\hat{Y}=1 \mid S\neq 1\right]}{P\left[\hat{Y}=1 \mid S=1\right]}\geq 1-\varepsilon \tag{1}$$

其中，$S=1$表示受保护属性的特权组，$S\neq 1$表示非特权组，$\hat{Y}=1$表示预测结果是积极的，差异影响的值越大表示算法越公平。与差异影响相似的公平性测度还有分类任务中的人口均等（demographic parity），但是判断的标准是两类群体预测概率的差值，而不是比率。除此之外，算法公平性的常见测度还包括监督学习任务中的机会均等（Equal opportunity）、个体公平（Individual fairness）等。值得注意的是，在算法设计过程中，算法公平性安全性的提升会带来算法高效性的下降，无法实现多目标同时优化。因此，可信算法需要在多个评估指标中取得平衡。

五、基于全国数据交易链的 PDCA 模型实现路径

5.1 全国数据交易链

全国数据交易链是指基于区块链技术的一种数据交易平台。它通过将数据商品化，实现数据的交易和流通，从而推动数据资源的优化配置和价值挖掘。全国数据交易链的核心理念是利用区块链技术的去中心化、安全、可追溯等特点，构建一个公平、透明、可信的数据交易环境。

具体而言，各地业务系统将各种业务数据传递、存储到地方数据中心，通过数据交易链，数据流转于区域数据交易所、行业数据交易所、数据资产交易中心以及上海市数据交易所等区域节点和行业节点，数据提供商在数交所平台登记确权，对数据进行链上授权，数据需求方在数交所平台通过链上查询进行数据交易。打造“平等互信、可信交易、自主可控、安全高效、监管追溯、绿色交易”的数据产品智能交易服务市场新模式。

全国数据交易链的主要应用场景包括数据确权、数据交易、数据安全等方面。通过区块链技术的应用，全国数据交易链能够解决数据交易中的信任问题，降低数据交易的成本，提高数据交易效率，保护数据所有者的权益，推动数据资源的流通和共享。

总体而言，全国数据交易链是我国在区块链技术应用方面的一次重要尝试，规划以数据交易所为枢纽的标准化全国数据产品智能交易服务新市场，有助于推动我国数据资源的发展，提升我国在全球数据交易市场的影响力。

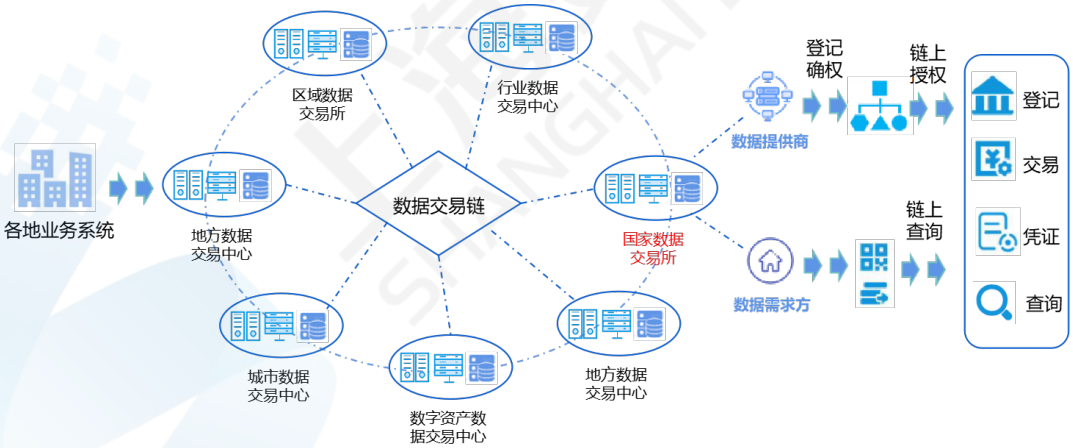

图 7 全国数据交易链

5.2 面向场景的数据要素安全交易体系设计

2022 年 12 月 19 日，中共中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”），要求建立数据可信流通体系，增强数据的可用、可信、可流通、可追溯水平，实现数据流通全过程动态管理，在合规流通使用中激活数据价值。

为了响应国家对于数据要素价值释放的要求，数据要素信任交易体系由智能撮合中心和安全学习与计算算法资源池两部分组成。其中，数据要素智能撮合中心在数据要素市场信息异质不对称性限制下实现供需双

方最优匹配，提升买卖双方合约订立的可信性。安全学习与计算中心为数据要素的合约履行提供攻击鲁棒性、防窃取能力和结果公平性的多方安全学习与计算方法支撑。

（1）撮合数据要素的提供方和潜在需求方是实现数据市场价值的重要途径。

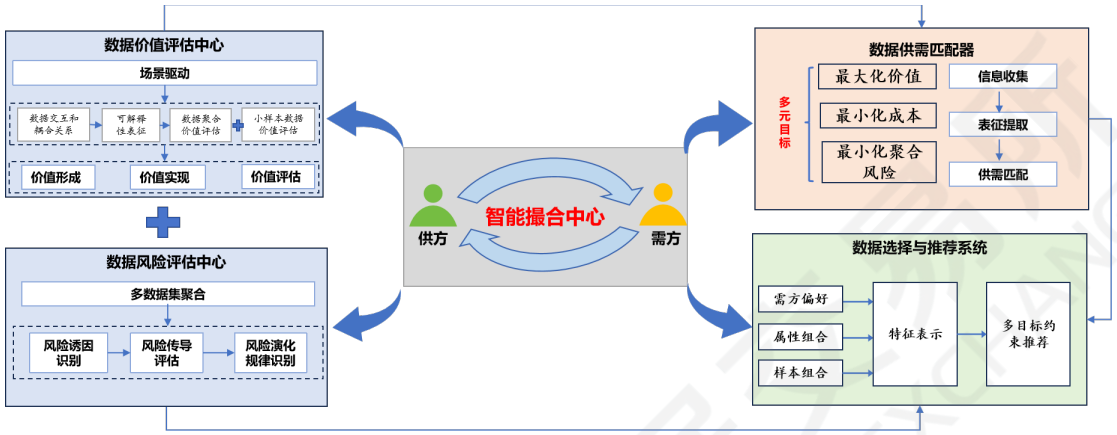

图 8 数据交易平台智能撮合中心框架

不同于传统商品要素，数据要素具有情景性、多态性、动态性以及内部结构复杂等特点，这些特点的交织导致数据价值评估难。随着数据交易体系的不断完善，互联网以及大数据技术的不断发展，以数据价值评估、数据风险评估、数据供需匹配以及数据选择与推荐方法等为代表的一系列相关理论与方法已经在数据智能撮合中得到了应用，极大提高了数据流通效率，促进了数据共享与数据价值发挥。基于此，智能撮合中心由数据价值评估中心、数据风险评估中心、数据供需匹配器和数据选择与推荐系统构成，提高数据要素流通撮合效率，促进数据共享与数据价值发挥。

数据价值评估中心提供场景驱动的多数据聚合的价值适应性评估功能，是数据匹配和推荐的基础。在不同场景下数据价值具有相对性，各项数据之间的交互和耦合关系将影响数据聚合价值。考虑离散数据、文本数据、图结构数据和图像数据等复杂异构数据之间的相关性和冲突性，识别不同数据集特征之间的交互和耦合关系。基于特征之间交互和耦合关系，实现多视角学习的多数据集可解释性表征。通过识别数据之间的共识信息和互补信息，提供面向场景的数据聚合价值适用性评估功能。针对交易场景中平台提供样本数据少等问题，提供针对性的小样本场景下多数据特征组合价值映射评估功能。总体实现基于多数据集聚合的数据价值形成、数据价值实现、数据价值评估等数据价值化路径。

数据风险评估中心提供多数据集聚合时风险涌现及风险传导现象评估功能，能够有效预警隐私泄露等问题，切实保障数据聚合的准确性、高效性和稳定性。针对多数据集聚合时各属性之间的互补式协同交互，识别产生隐私泄露风险、商业秘密风险及国家安全风险等的致因属性微观交互机制与宏观风险涌现间的关联关系，提供多数据特征组合数据风险诱因识别方法。针对同领域交易和跨领域交易情境下多数据集聚合时多类型风险耦合性和外溢性，提供基于解耦学习的多数据集聚合的风险传导评估。考虑数据风险的动态特征，从短时性风险和持续性风险视角，识别多数据集聚合产生的多元数据的风险演化规律，评估和管控“数据化合反应”产生的潜在风险。

数据供需匹配器实现考虑供需双方效用的数据要素供需智能匹配，促进供需双方交易撮合。数据交易平台中存在海量的数据集以及各种类型的需求者，而平台的目标是为需方匹配满足其需求的数据集。利用供方数据集的元数据、标题、描述、在线评论等以及需方需求描述等文本信息，从语义层、表示层以及情景应用层三个维度提取数据集和需方的表征，达成预算和风险控制边界约束下的数据要素供需匹配。其中，考虑供需双方信息时变性的特点，动态评估需方数据需求与供方服务能力，提供最大化价值、最小化成本、最小化聚合风险多元目标组合约束情景下数据要素智能匹配优化功能。

数据选择与推荐系统针对买方数据需求不确定或模糊的情形，提供多元目标约束下的数据精准推荐功能，是提高买卖双方交易意愿的重要数据交易服务。考虑数据产品各维度属性的价格、需求方预算约束、供给方风险约束、以及需求方的偏好，提供基于需方偏好和数据组合的数据精准推荐框架。具体包括，面向需方偏好预测，基于需方和数据交易平台之间查询、点击和购买等多类型交互行为数据以及数据产品的元数据、标题、描述等信息，提炼需方多维度偏好的知识图谱表示，分析需方感兴趣的数据类型、属性以及规模等。面向属性组合推荐，结合数据要素各属性的价值、风险、价格特征，基于群组变量选择方法，提供不同成本和风险边界范围内的数据属性组合与表示功能，联合需方偏好表征与数据属性表征的属性组合推荐功能。面向样本组合推荐，考虑数据样本的多样性、代表性、价值性、风险性，利用高阶关联和迭代寻优等策略，提供不同成本和风险边界范围内的数据子集选择和表示功能，联合需方偏好表征与数据子集表征的样本组合推荐功能。

（2）数据要素使用过程中的安全学习与计算是激活数据价值的关键手段。

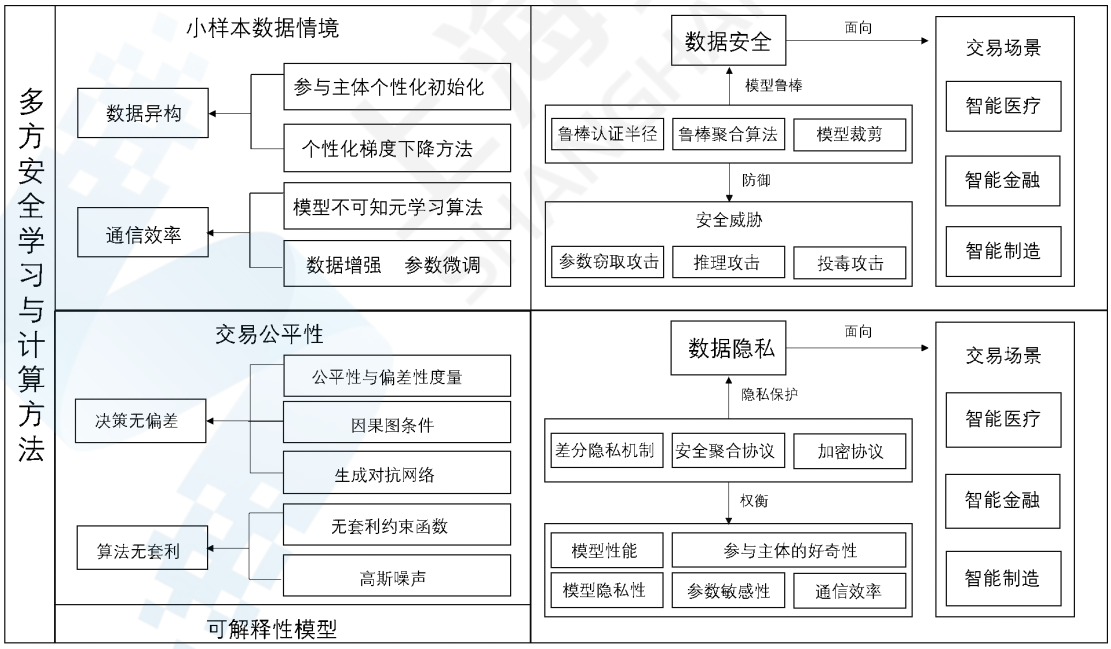

图 9 安全学习与计算算法资源池

数据要素流通涉及的场景复杂，常面临有效数据样本不足以及参与主体非法攻击、窃取与合谋等情景，引发准确性、安全性、隐私性和公平性等方面的严重缺陷，从而为数据要素的可信流通带来极大挑战。按照“无场景不交易”和“数据可用不可见”的现实要求，以联邦学习、多方安全计算为代表的隐私计算技术是一类

能够保障数据要素隐私和安全，实现数据要素流通使用的典型技术。因此，具有攻击鲁棒性、防窃取能力、公平性的安全学习与计算算法资源池是保护数据安全学习与计算的技术基石。

具有攻击鲁棒性的多方安全学习与计算方法保障了算法的安全性。数据要素流通的过程中涉及多方主体参与，参与学习的恶意主体可能通过对学习模型或是计算过程发起对抗性的攻击，导致学习模型的性能下降。在应对不法参与主体的攻击时，大多数多方安全学习与计算方法针对某一种特定攻击方法进行防御，而在真实数据交易场景中，非法参与主体的攻击行为通常是未知的且不同参与主体的行为、数据及模型可能均有差异，这可能导致防御方法无法同时保障参与主体应对各种可能攻击的鲁棒性。针对投毒攻击、后门攻击、拜占庭攻击等不同攻击形式及攻击强度对模型完整性的影响，提供基于参数偏差效应的样本级多方安全学习与计算方法的鲁棒认证半径，划分多方安全学习与计算方法的安全边界。利用客户端参与多方学习和计算的历史行为数据，基于生成式对抗网络分析历史梯度特征，基于融合同态哈希函数映射与梯度相似度识别恶意客户端。基于鲁棒认证半径与客户端恶意水平，提供不同客户端模型梯度在服务端的聚合策略，包括权重更新策略、梯度压缩策略和噪声引入策略，同时基于非法攻击在模型参数中的累积效应，确定模型梯度的最优迭代策略和最佳聚合时机。

具有防窃取能力的多方安全学习与计算方法提升了算法的隐私保护能力。在数据要素流通的过程中，在交易实施环节，好奇的参与主体可能发动隐私窃取攻击，通过逆向工程等手段获取数据要素的信息或是模型的参数等敏感信息，导致数据交易参与主体的利益损失。利用多方安全学习与计算主要通过多轮交互收集的模型参数数据的特点，推理出拟窃取的机密信息的攻击策略，基于训练样本的统计特征、分布规律、样本规模等与模型参数之间的关系，归结模型参数规模及交互次数对样本统计特征、分布规律的推理能力的影响。以此为突破口，从模型参数和训练样本两个视角提供有效的防窃取策略。一是面向模型参数的防窃取策略，选择模型参数的压缩策略以减少交互参数的规模，采用最优训练策略以降低参数交互的次数，优化模型参数的分配策略以控制客户端对全部参数的访问，利用基于差分隐私技术的参数扰动方法以减少真实参数信息的泄露。二是面向训练样本的防窃取策略，寻找数据样本和数据属性的最优分割策略，以降低恶意方分析数据分布、数据统计特征的能力，基于不同样本和属性分割策略，提供本地迭代与多方迭代的优化功能，减少客户端之间的交互次数。

输出结果公平的多方安全学习与计算方法实现了数据要素交易公平性。在数据要素可信流通过程中，由于大多数的数据流通使用通过既充当交易的组织者又充当裁判的数据交易平台进行，如果出现平台与买方或卖方合谋，交易的公平性将难以保证。针对算法歧视与合谋套利等危害交易公平性的行为，现有方法主要考虑到数据要素本身作为一种特殊的商品具有易复制性和易追踪性等特点，通过因果关系、人机协同、贡献度量等方法实现决策无歧视和算法无套利，然而忽视了数据持有方的数据成本和模型可解释的问题，从而制约了数据要素流通场景下交易公平性的保障效果。针对算法的黑箱性以及算法决策结果可能存在的不公平性，提供有效的决策结果无歧视策略、数据交易无套利策略和决策结果透明化策略，增强了买卖双方互信程度。根据模型结构与训练数据对决策结果有偏性的影响机制，提供人机协同的模型参数分发、预测结果重标定策略，实现最小决策偏差的迭代优化。针对数据要素交易中的算法恶意合谋套利问题，最小化多方安全学习与计算方法的合谋机制、潜在套利类型及风险，提供有效控制合谋的算法参数约束策略，并进行典型套利威胁

下的算法选择与优化。针对多方安全学习与计算方法的透明性问题，结合注意力机制、生成式对抗网络、反事实推断学习等技术，实现可解释性及事后可解释性的多方安全学习与计算方法。

5.3 面向数据要素流通全过程的追溯体系设计

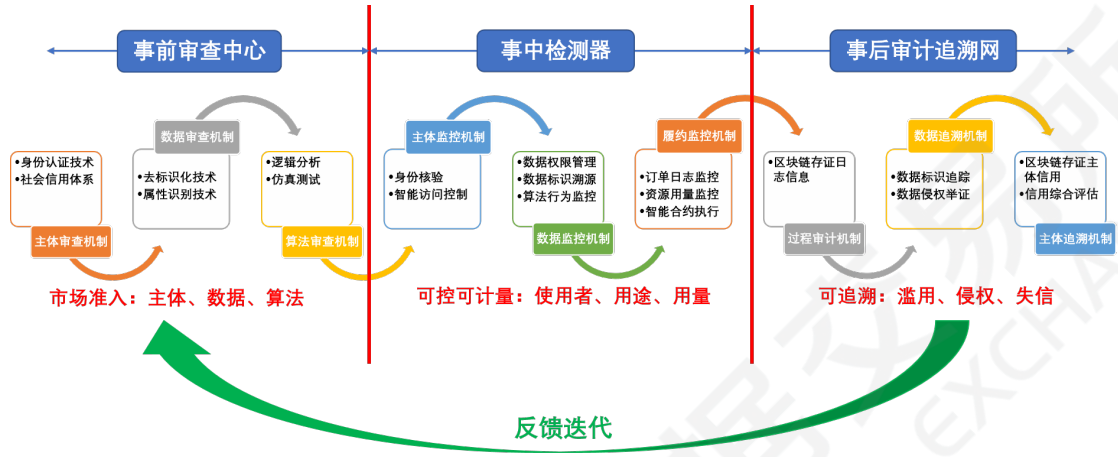

图 10 数据要素流通全过程追溯体系

2021 年 3 月发布的《“十四五”规划和 2035 年远景目标纲要》中明确提出，要培育规范的数据交易平台和市场主体，发展数据资产评估、登记结算、交易撮合、争议仲裁等市场运营体系。然而，随着数据要素市场化发展提速，数据要素呈现形态多源异构、流转链条增长、参与主体多样等特点，叠加自身的可复制性、非排他性等属性，带来了数据来源难确认、数据流向难追踪、使用范围难控制、流通互信难保障等可信流通问题。对数据要素可信流通全过程进行有效审查、监督、跟踪、追溯，成为保障各参与主体合法权益、激发数据要素市场活力的关键。面向数据要素可信流通全过程的追溯体系包括事前审查中心、事中检测器和事后审计追溯网。

事前审查中心提供入场交易的主体身份认证、数据可溯管理、算法安全评估三大功能，确保进入市场的主体、数据、算法安全合规。面向主体审查，针对参与主体身份多元和资质参差等特点，利用“数字+生物”主体身份认证技术和社会信用体系，提供“机器审查+人工复核”的双重协同主体安全审查，保障入场主体可信。面向数据审查，能够基于去标识化与敏感属性识别技术管控敏感数据，基于数据标识技术实现多源异构数据产品互认连通，提供数据产品质量动态管理能力，确保数据产品的合规性、完整性、可追溯。面向算法审查，根据算法本体、设计过程和决策结果等维度，评估面向全生命周期过程的算法影响，提供基于逻辑分析与仿真测试多路协同的算法审计功能，确保算法产品的合规性、高效性和负责任。

事中检测器能够有效监控合约签订与履行中的失信行为，确保数据要素流通使用过程安全可信。对于数据买方，存在非法滥用和越权访问数据等风险。针对数据非法复制、窃取、备份等数据滥用行为，提供面向计算资源用量异常检测的自动感知功能，实时监控数据再次流转。针对买方二次转卖、共享数据等数据越权访问行为，根据数据访问权限范围，实现身份认证和智能访问控制相耦合的交易主体访问权限管理。对于数据卖方，存在异常供给数据的风险。针对卖方在履行合约时可能提供低质量数据、污染数据，甚至恶意窃取其他参与方数据等行为，提供数据质量和算法训练过程智能化监控功能，具体包括首先利用数据标识技术等

数据溯源方法验证数据真实性，随后根据“各方日志审计-每轮攻击检测-交付性能验证”路径实现全方位算法训练安全性实时检测。交易合约作为约束买卖双方的重要凭证，合约履行监控是保障交易合规安全的关键，提供基于计算日志与资源用量协同的计算用量异常检测，利用计算合约自动审核执行，实时感知计算全流程数据流通态势。

事后审计追溯网能够定位异常节点，为数据要素流通使用全过程提供溯源凭证，确保交易完成后的不可抵赖性。以全国数据交易链为核心，提供面向事前审查和事中检测的数字存证策略，实现基于数字存证技术的数据要素可信流通事后审计与追溯。对于过程审计，面向数据流通事前审查、事中检测等全过程日志信息，提供基于区块链的数字存证策略，利用存证信息审计主体、数据、合约和算法安全合规。对于数据追溯，面向流通数据本体，实现基于数据标识和关联技术的数据溯源追踪，应用数据水印、数据血缘追踪等技术对数据二次流通、转卖等侵权行为进行查验取证。对于主体追溯，面向交易主体信用行为，结合社会信用体系与区块链技术，实现市场主体交易行为信用评价的链上存证，提供数据信用综合评估服务，确保交易主体信用等级信息可追溯。

六、基于 PDCA 模型的保障体系

数字经济逐渐进入高质量发展时期，数据要素市场对数据安全愈加重视。数据要素在入场前的合规审查、流通使用过程中的用途用量控制、流通使用后的争议解决等问题，对数据要素的安全治理和安全保护提出更高要求。因此，本文从“事前审查→事中监控→事后审计”的视角，对国内外现有数据要素可信流通监督监管策略的制度与政策和理论与技术进行总结梳理。目前国内外相关工作主要集中在制度与规范建设和理论与技术保障两个方面：一方面通过政策、制度、标准制定明确数据流通使用安全风险管理要求，另一方面通过理论与技术手段解决数据流通使用安全风险管控问题。

6.1 面向制度与规范约束的 PDCA 监管策略分析

近年来，我国数据要素市场发展态势十分迅猛，市场规模迅速扩大。《中国数据要素市场发展报告（2021-2022）》7表明，2021 年我国数据要素市场规模达 815 亿元，预计“十四五”期间市场规模复合增速将超过 25%。为防范数据要素市场安全风险事件，国家出台一系列政策文件和规章制度统筹数据要素安全风险管理。2021 年 3 月发布的《国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》8中明确提出，要培育规范的数据交易平台和市场主体，发展数据资产评估、登记结算、交易撮合、争议仲裁等市场运营体系；2021 年 11 月，工业和信息化部发布的《“十四五”大数据产业发展规划》9中不仅再次提到了有关数据要素市场建设的内容，还围绕加快培育数据要素市场、发挥大数据特性优势、夯实产业发展基础、构建稳定高效产业链、打造繁荣有序产业生态、筑牢数据安全保障防线六个方面提出了重点任务；2022 年 12 月 2 日，中国中央 国务院印发《关于构建数据基础制度 更好发挥数据要素作用的意见》，强调完善数据全流程合规与监管规则体系，从全流程治理与创新监管机制等方面入手，提出底线可守的数据要素安全治理制度。

6.1.1 事前审查

事前审查是数据要素流通使用安全风险管控的前提，主要是指市场或市场管理者在交易前对数据交易市场的参与者和数据产品依照相关的法律法规进行审查，实现数据“上市有审核，采买有资质”。在国家层面，《数据安全法》中明确规定了数据交易服务机构应审核交易双方的身份、交易数据内容、数据安全风险，并留存审核、交易记录。在地方层面，天津市出台了《天津市数据交易管理暂行办法》，其中第二章和第三章分别对数据交易主体和交易数据做出一系列明确要求。在行业内部，通过制定措施保证数据来源合规可信、数据质量安全可控，例如，贵阳大数据交易所发布的数据交易规则体系10，就包含了《数据交易合规性审查指南》、《数据交易安全评估指南》、《数据商准入及运行管理指南》等，以保障数据要素流通使用过程中交易主体、交易对象可信可控。但在数据分级分类管理、数据确权授权等方面的法律制度有待进一步完善。例

[7] 国家工业信息安全发展研究中心，北京大学光华管理学院，苏州工业园区管理委员会，上海数据交易所，《中国数据要素市场发展报告（2021-2022）》，2022 年 11 月 25 日发布

[8] 《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》，2021.3.11，http://www.gov.cn/xinwen/2021-03/13/content_5592681.htm，访问时间 2023.2.7

[9] 国家工业和信息化部（工信部规〔2021〕179 号），《“十四五”大数据产业发展规划》，2021.11.15

[10] 贵州全国首发数据交易规则体系，2022 年 5 月 27 日，http://www.guizhou.gov.cn/home/gzyw/202205/t20220529_74403217.html?isMobile=false，访问时间 2023.2.18

如，《数据安全法》虽然明确提出国家将对数据实行分级分类保护，但仅作出了一般性规定，缺乏详细的分级分类体系和相关的实施细则，不同区域、不同部门不统一的程序标准容易导致数据准入与监管产生冲突；在立法层面《数据安全法》和《个人信息保护法》虽然解决了数据的国家主权和人格权的问题，但是数据的财产权问题尚未在法律层面有明确定义，其中数据要素的可复制性、不确定性等独特特征是数据产权制度体系建立的难点，使对参与交易的数据源的审查带来了操作上的困难。

6.1.2 事中监控

事中监控是数据要素流通使用安全风险管控的基础，目的是对数据使用的用途、用量加以控制，约束交易主体行为，监督交易订单合规履行。在《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》中，提出要建立合规高效的数据要素流通和交易制度，完善数据全流程合规和监管规则体系，建设规范的数据交易市场。各地方政府已陆续出台相关政策，促进数据要素安全可信流通。北京发布《北京市数字经济促进条例》11，要求完善数据分级分类、安全风险评估和安全保障措施，建立数据治理和合规运营制度，结合应用场景对匿名化、去标识化技术进行安全评估，开展数据安全方面的标准认证。上海市出台《上海市数据条例》12，支持数据交易服务机构有序发展，要求数据交易服务机构应当建立规范透明、安全可控、可追溯的数据交易服务环境，制定交易服务流程、内部管理制度，并采取有效措施保护数据安全。贵阳大数据交易所发布的《数据交易合规性审查指南》也包含了对交易合同内容、交付方式进行合规审查，同时还提供了《数据产品成本评估指引 1.0》、《数据产品交易价格评估指引 1.0》、《数据资产价值评估指引 1.0》，为数据交易提供价值评估和价格依据。但在定价机制、数据交易立法上还存在明显的欠缺。目前不同的数据交易平台的价格机制不透明，例如，某平台“省级业务平台数据服务”标价 351.56 万元/次，而“算力资源服务（云计算服务）”标价 0.01 元/次。因此，需要完善、统一数据流通定价规则，规范数据消费单位和消费方式，防止定价过于随意。在立法方面，有关数据要素流通使用的法律散落在《民法典》《个人信息保护法》《数据安全法》《网络安全法》《反垄断法》《反不正当竞争法》，还没有一部关于数据要素流通交易的法律，相比之下，美国 2014 年就通过了《数据经纪商问责制和透明度法案》，2019 年通过了《2019 年数据经纪商法案》，要求数据经纪商明确数据来源和类型，使用、保存和分发数据的方式，允许消费者访问和修改数据的范围，消费者退出数据销售或共享的方式等。

6.1.3 事后审计

事后审计是数据要素流通使用安全风险管控的关键，目的是解决交易后的争议问题。中共中央 国务院印发《关于构建数据基础制度 更好发挥数据要素作用的意见》中就数据要素市场的信用体系，提出需要配套建设交易仲裁机制，对数据交易主体的信用进行管理和评价，在数据要素市场形成诚信、互信、可信的交易生

[11]《北京市数字经济促进条例》，2022 年 11 月 25 日北京市第十五届人民代表大会常务委员会第四十五次会议通过，http://www.beijing.gov.cn/zhengce/gfxwj/sj/202212/t20221214_2878614.html，访问时间 2023.2.7

[12]《上海市数据条例》，2021 年 11 月 25 日上海市第十五届人民代表大会常务委员会第三十七次会议通过，https://www.shanghai.gov.cn/nw12344/20211129/a1a38c3dfe8b4f8f8fcba5e79fbe9251.html，访问时间 2023.2.7

态。在企业内部，北京国际大数据交易所发布《北京数据交易服务指南》13，推行数据交易保护义务衍生的原则，就交易中规定的使用范围和禁止用途进行保障，并设立数据要素产权知识保护体系，建立买卖双方争议解决机制。贵阳大数据交易所发布的《数据交易合规性审查指南》也包括交易后对场景应用、新增衍生数据产品进行合规审查。但在数据泄露通知制度、数据监管权限方面还需持续完善。虽然《网络安全法》制定了数据泄露通知制度的相关要求，但是需要向用户告知的特定情形、告知用户的时限和方式、数据泄露的补救和惩戒措施、制度适用的主体范围等制度要素没有做出明确规定，缺乏一定的可操作性。在我国，数据监管由网信部统筹，行业各部门分别监管，但实践中各数据监管部门、纠纷仲裁机构权责划分不明确、责任互相推诿的问题屡见不鲜，应完善数据监管、纠纷仲裁相关制度，明确相关权力与职责，形成行业自律与政府监管双重安全保障。

6.2 面向理论与技术支撑的 PDCA 监管策略分析

6.2.1 事前审查

在参与者资格审核方面，通常使用身份认证与控制技术保障交易主体的资质安全，确保数据供方和需方提供的身份信息真实可靠。传统的身份认证主要有基于标记识别的身份认证、基于生物特征的身份认证和基于密钥的身份认证等方式，但存在着密码泄露、伪造生物特征等风险。近年来，区块链技术开始应用于身份认证领域，区块链具有去中心化、不可篡改的优势，可为主体资质安全提供技术支撑。例如，在物联网数据市场，利用区块链、分散标识符（Decentralized Identifier，DID）进行主体验证，其中每个主体持有一个独特的 DID，通过在客户端验证 DID，确保平台上的交易主体身份得到认定；在权限访问控制上，TID-MOP 安全体系框架[44]在技术保障方面实施数据交易申请的安全管控，通过集中监控运维和访问权限管理重点关注交易主体合规资质的评估。

在审核数据要素的合法性、合规性、真实性方面，去标识化技术、敏感数据探测技术、完整性技术为数据产品的安全准入提供了技术保障。去标识化技术通过对原始数据进行去标识化处理，降低数据集中的信息与信息主体的关联程度，主要包括数据统计技术、抑制技术、匿名化技术、假名化技术、泛化技术、随机化技术等，不同的去标识化技术具有不同的特点，数据供方可以根据不同交易数据的特点、保密级别，选择合适的数据去标识化技术，从而确保数据产品可以进入数据要素市场。针对数据产品中包含敏感信息的问题，采用面向结构化数据集的敏感属性自动化识别与分级算法，利用信息熵定义属性敏感度，通过对任意结构化数据集的敏感属性进行识别和敏感度量化，可以实现敏感属性的分级分类。针对数据质量问题，数据完整性技术一方面可以保障参与交易的数据质量，另一方面可以保障数据不被恶意篡改，其中密码学技术和数据副本策略是两种传统的数据完整性技术。密码学技术利用消息认证码和哈希树等生成数据签名信息，防止数据被伪造；数据副本策略则是通过损失存储空间来保障数据完整性。实践中，一般综合利用两种方法确保数据质量安全。

[13] 北京国际数据交易联盟，《北京数据交易服务指南》，2021.3.31

6.2.2 事中监控

区块链技术和隐私计算技术体系是保障数据流通使用过程中计算环境安全、算法安全和数据隐私的有力手段，也是监控交易撮合可信的可行技术。

例如，在监控交易撮合可信方面，Tan 等人[45]提出了一种考虑信用管理的基于区块链的分布式交易机制，只有当用户的信用评分不低于阈值时，才能允许用户参与分布式交易；Gupta 等人[46]提出了一个新的区块链框架 TrailChain，该框架使用水印生成可信交易跟踪，通过建立检测市场内和市场间任何未经授权的数据转售的机制，实现对跨越多个分散市场的数据所有权的溯源跟踪。

在保障计算环境安全方面，可信执行环境(Trusted execution environment，TEE)可将敏感计算与其他进程（包括操作系统、BIOS 和 hypervisor）隔离开来，通过芯片等硬件技术并与上层软件协同对数据进行保护，且同时保留与系统运行环境之间的算力共享，主要代表性产品有 Intel 的 SGX、ARM 的 TrustZone 等；基于可信执行环境和区块链技术，Dai 等人[47]构建了一种新的数据交易生态系统，其中数据代理和需方都无法访问供方的原始数据，而只能访问所需的分析结果，安全执行环境起着保护数据处理、源数据和分析结果的作用。

在算法安全及隐私保护方面，已经取得了丰富的研究成果，例如，区块链中可以采用同态加密、零知识证明等技术对隐私数据进行加密以达到保护隐私数据的目的；Zheng 等人[48]针对供应链金融信用体系中的征信数据隐私保护问题，提出了一种基于区块链的共享交易信息访问控制和管理模型，通过共识机制，实现了共享数据链的访问控制和可追溯性管理；Zhang 等人[49]提出了一种基于移动边缘计算的联邦学习框架 FedMEC，将模型划分技术和差分隐私技术集成在一起，防止局部模型参数的隐私泄露；郑婷一等人[50]还提出了一个由监管体系、核心技术和模式创新三部分组成的保障平台数据与算法安全的技术生态体系架构。

6.2.3 事后审计

事后审计主要包括交易信用审计和交易安全审计。交易信用审计主要对是否存在侵权和违规行为进行认定、追责,并建立一种有效的信用评价机制。例如，可以利用区块链可溯源、抗抵赖等技术特性,提出参与者向智能合约支付一定数量的押金作为对潜在违约者的惩罚和对被违约者的补偿，在规定期限后，由智能合约根据合约履行情况执行交易结算，并根据参与者本次的表现自动刷新其信用评分。还可以利用边合约机制，建立一种基于区块链技术的交易纠纷仲裁机制，不仅可以解决交易双方的合同争议问题，还能验证、追溯交易数据的完整性和价值。可以设计一种信誉机制设计方案，以鼓励供方尽可能多地降低机会主义，防止交易对需方没有价值的数据产品。区块链技术的应用不仅能保障每笔交易的记录安全，还为交易安全审计提供了便利。例如，Kefeng 等人[51]设计了一个基于区块链的云数据审计方案，提出了一个分散的审计框架来消除对第三方审计者的依赖，保障了数据审计的稳定性、安全性和可追溯性的同时，还能更好地协助用户以验证云数据的完整性。表 6 简要汇总了国内外数据要素流通使用安全风险及其主要应对策略。

表 6 数据要素流通交易使用安全风险应对策略

业务周期 / 应对策略	交易申请	交易磋商	交易实施	交易结束
政策、制度	交易主体资质审核、数据产品合规性审查	交易合同审核	交易环境安全风险评估、算法安全风险评估、交易服务管理制度	登记结算、争议仲裁
理论、技术	身份认证技术、数据去标识化技术、敏感数据探测技术、数据完整性技术	区块链智能合约、分布式交易机制	P2P 网络技术、区块链、智能合约、安全多方计算、差分隐私、可信执行环境、联邦学习	分布式交易机制、云数据审计、边合同机制

6.3 管理与技术协同的数据要素可信流通机制

图 11 展示了本文提出的事前事中事后全链路数据要素流通使用安全风险应对策略框架，从数据要素流通使用全过程视角，针对事前、事中、事后三个不同阶段，分别制定事前审查体系、事中监控体系和事后审计体系，规范数据安全有序流通使用。

图 11 事前事中事后全链路数据要素流通使用安全风险应对策略流程图

6.3.1 事前事中事后全链路监管机制

(1) 基于人机协同的事前审查体系

事前审查的目的是期望在交易申请阶段能够确保参与交易的主体可信、数据可信、合约可信等，如图 12 所示。交易主体审查旨在审查数据流通使用主体资质的安全风险和合规性，构建交易主体账户注册登记流程，设计面向账户登记信息真实性的机器审核与人工复核配套验证方案，保证交易平台、流通交易过程中的经手方以及机构或个人等市场主体信息可追溯，实现交易主体可信。交易数据和算法审查即检验采集存储的数据要素安全风险，包括数据完整性、真实性、可交易性，数据获取渠道的合法性，以及数据是否对个人信息进行去标识化处理，保障数据的可交易以及合法合规。交易合约审查目的在于审查数据要素的使用场景、

数据质量、数据价值、可定价要求和数据更新能力，需要面向不同应用场景制定禁止交易数据目录，建立数据产品上架交易标准规范，构建规范化的交易合约上架流程和合规审查流程，实现交易合约可信。

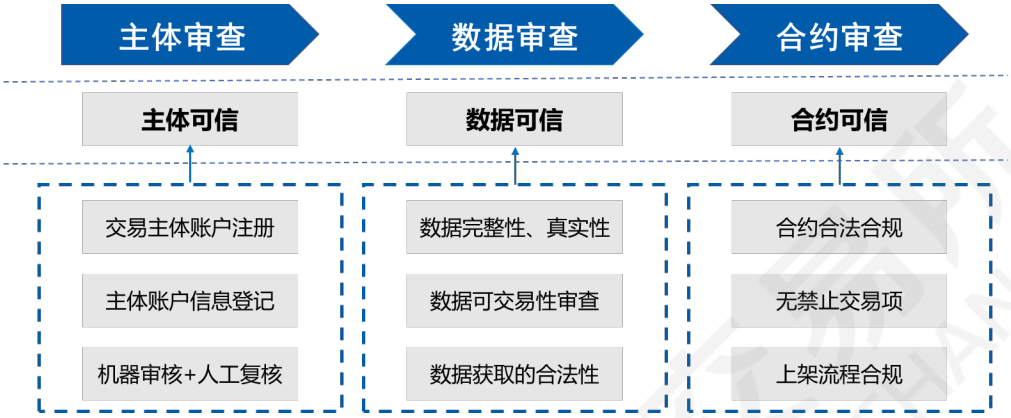

图 12 事前人机协同审查体系

(2) 基于智能监控管理的事中监控体系

事中监控的目的是保障数据要素流通交易在磋商阶段和实施阶段安全可信，包括交易主体监控管理、合约磋商监控管理、算法行为监控管理和订单履行监控管理，如图 13 所示。交易主体监控管理聚焦于交易主体识别管理，通过设计基于智能识别技术的交易主体身份与合约核验机制，确保合约双方的签名信息、合约内容的哈希值信息、私钥管理信息等合约信息的可追溯，实现数据使用者可控。合约磋商监控管理，基于公平交易原则、供需匹配效率最大化原则，通过设计具有隐私保护的自动匹配技术和智能合约技术，保障交易双方的合约符合市场预期和国家相关政策法规。算法行为监控管理，通过构建模型算法评估体系，设计算法行为监控方案，确保数据导入、数据预处理、模型训练、结果发布等流程规范可信、使用过程可追溯、资源消耗可度量，实现数据用途、用量与合约一致，保障数据加工使用安全风险可控。订单履行监控管理，建立数据传输接口备案制度，通过动态监控交易主体履约行为，包括感知监控数据流转、验证数据完整性和一致性、资金流审核，保证订单完全履行，并能对订单信息、供需方及交易平台信息、交付结算信息等履约过程产生的数据信息的可追溯。

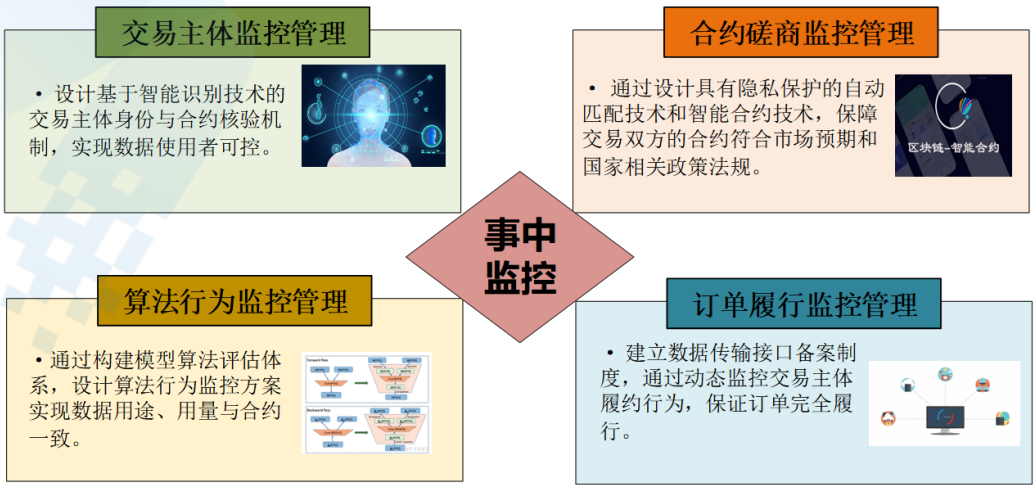

图 13 事中智能监控管理体系

(3) 基于区块链存证的事后审计体系

事后审计是防止数据在交易结束后可能面临的安全风险，集中在防止数据滥用、数据侵权和主体失信三个方面，如图 14 所示。在防止数据滥用方面，设计基于数据链上存储信息的交易审计机制，以交易结束后链上存储的合约信息和交易信息为基础，构建智能交易审计核验指标测算体系，设计链上资源滥用情况的监控和识别方案；制定数据销毁审查机制，杜绝数据产品倒卖风险，保证交易数量、异常交易用户、异常合约部署、数据销毁过程等审计信息可追溯。在防止数据侵权方面，制定数据交易侵权行为的举证流程机制，基于数据侵权行为链上链下线索搜寻，构建数据侵权的链上链下查验体系，保证对侵权行为信息来源的可追溯。在防止主体失信方面，建立数据交易结束后的链上存储信息的信用管理机制，构建基于数据市场主体的信用评价指标体系，设计市场主体交易行为信用评价的链上存证方案，保证对数据供方、数据需方、交易平台等数据市场主体信用等级信息的可追溯。

图 14 事后区块链存证审计体系

6.3.2 管理与技术协同的监管体系

支持数据要素安全有序流通使用需要构建一个全流程合规可信体系，其建设过程是一个复杂的系统工程，实现路径有赖于管理制度与技术支撑的相互保障和综合作用。图 11 展示了本文提出的管理与技术相互协同的数据要素流通使用合规可信体系及实现路径。图 15 中，①表示交易申请阶段参与主体注册及对应的管理机制、技术支撑。类似地，②表示交易撮合阶段，③表示交易实施阶段，④表示交易结束阶段，以及各自对应的管理机制和技术支撑。

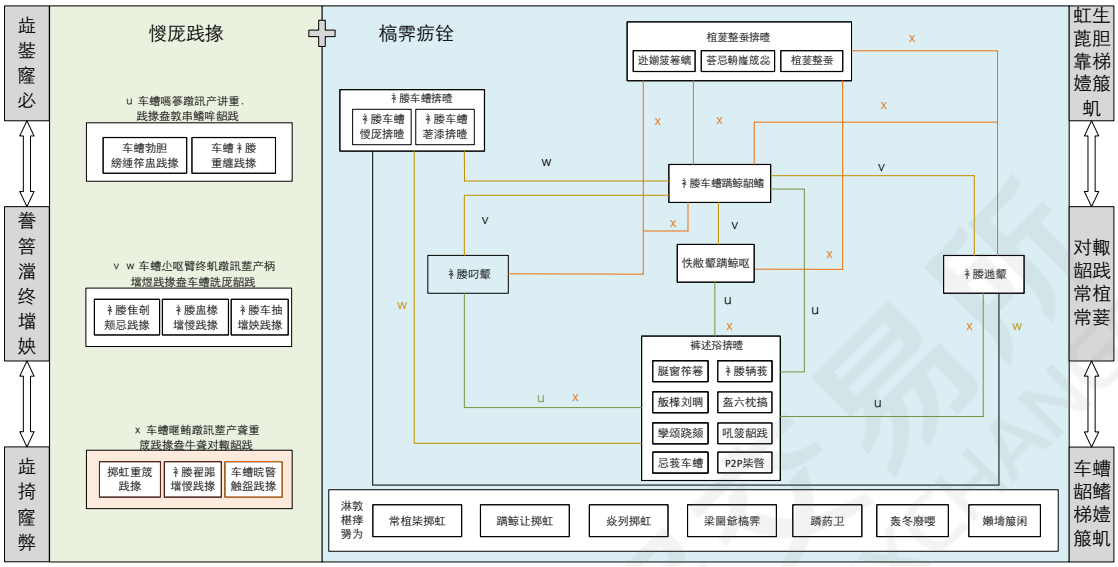

图 15 管理与技术相互协同的数据要素流通使用合规可信体系及实现路径

(1) 管理制度与技术支撑相互协同的数据要素流通使用全流程合规可信体系

管理制度与技术支撑相互保障的数据要素流通使用全流程合规可信体系包括合规可信制度体系、合规可信技术体系以及管理制度与支撑技术协同方案。数据要素可信流通使用制度体系包括事前审查制度、事中监控制度、事后审计制度等；技术体系包括数据交易系统技术、区块链系统技术、跨隐私平台的联邦学习系统技术以及可信执行环境技术等；图 15 中标记的①~④展示了数据要素流通使用不同阶段的管理制度和技术支撑的协同方案。

具体而言，在数据流通使用的事前审查阶段，制定针对交易主体、交易数据和交易合约的审查制度，应对参与主体和数据采集安全风险；在技术上采用“机器审查+人工核验”方式保证审查流程合规可信，即对于资质信息、数据质量、交易条目等标准信息，如企业法人信息、营业执照、数据规模与量级、禁止交易数据清单等，采用基于机器学习算法进行自动审查与人工抽验方法；对于交易目的、数据来源等主观性较大的数据属性，采用人工核验方法。在数据流通使用的事中监控阶段，针对流通使用涉及的平台系统及软硬件、数据、云、网、端等环节制定安全保障制度，构建交易主体监控管理体系、算法行为监控管理体系和订单履行监控管理体系；在技术上设计基于智能算法支撑的保障体系，如基于智能识别技术的参与主体身份认证，保证参与主体可信；基于标识技术的数据权限管理方法，实现交付数据访问可控；面向数据用量异常检测的自动感知技术，监控数据合规加工使用；基于区块链技术的数据流通使用过程信息存证，保证数据流通使用全过程可追溯。在数据流通使用的事后审计阶段，制定数据滥用审计制度、数据侵权审计制度、主体失信审计制度，旨在确保数据流通使用全过程合规、争议可裁决、权益可保障；在技术上设计基于区块链存证信息的再审计体系，对数据流通使用全过程进行安全审计；基于数据标识和关联技术的数据追踪体系，对数据二次流通、转卖等侵权行为进行查验取证；融合交易主体信用评估制度体系与区块链可追溯技术，构建数据信用综合评估服务，推动数据流通市场公正可信发展。

(2) 数据要素流通使用全流程合规可信体系建设方案

数据要素流通使用全流程合规可信制度体系既有指导全国一体化实施数据要素流通使用的宏观基础制度，又有地方政府指导本地区实施数据要素流通使用的中观制度，同时还有数据要素交易机构实施数据要素流通使用的微观制度。在国家和地方层级的宏观制度、中观制度建设方案上，采用“自顶向下”的思路构建数据要素流通交易全流程合规可信基础制度体系。在地方和交易机构的微观制度、中观制度建设方案上，采用“自底向上”的思路，构建数据要素流通交易全流程合规可信运营制度体系。在安全可信制度的实施保障上，制定数据要素流通使用全流程合规可信制度体系培训政策、落实保障政策以及制度执行的监管政策，保障数据要素流通交易全流程合规可信制度有效落地。

数据要素流通使用全流程合规可信技术体系既包括国家支撑数据要素流通交易的全国一体化基础设施，又包括各类数据交易机构支持数据要素可信可控可计量流通交易的基础设施。在全国一体化基础设施建设上，基于“东数西算”等国家基础实施建设战略，厘清全国一体化数据中心、算力中心、算法中心、安全中心等安全可信基础设施与流通环境的建设需求，提出相应的建设方案，为数据要素流通使用提供安全可信流通环境、共性公共服务、绿色高效的算力保障 。在数据交易机构基础设施建设上，构建面向集合运算、联合建模及风险防控等功能的隐私协同计算平台，设计面向交易主体互信、数据登记互联、失信名单互通的跨链协同交易平台，为数据要素安全可信流通使用提供安全可信技术保障。在安全可信技术建设保障与互联互通上，建议国家开展相关技术攻关、基础理论探索等重点工程项目与专项行为计划立项工作，以重点工程项目与专项行动计划为牵引，建立国家、地方政府与交易机构共同投资建设的协同机制以及各类基础设施互联互通机制，建立安全可信、集约高效的全国一体化数据要素流通使用环境。

参考文献

[1]欧阳日辉 and 荆文君, 数字经济发展的“中国路径”：典型事实、内在逻辑与策略选择[J]. 改革, 2023(08): 26-41.

[2]曹明星, 数字经济下的数据要素治理与数字税收改革——基于“信用价值集聚生产”创新经济理论的初步探讨[J]. 税务研究, 2022(11): 36-42.

[3]洪永淼, 张明 and 刘颖, 推动跨境数据安全有序流动 引领数字经济全球化发展[J]. 中国科学院院刊, 2022. 37(10): 1418-1425.

[4]Turow J., Hennessy M. and Bleakley A., Consumers’ understanding of privacy rules in the marketplace[J]. Journal of consumer affairs, 2008. 42(3): 411-424.

[5]Kole S. R., Measuring managerial equity ownership: a comparison of sources of ownership data[J]. Journal of corporate finance, 1995. 1(3-4): 413-435.

[6]徐翔 and 赵墨非, 数据资本与经济增长路径[J]. 经济研究, 2020. 55(10): 38-54.

[7]Kallus N., Mao X. and Zhou A., Assessing algorithmic fairness with unobserved protected class using data combination[J]. Management Science, 2022. 68(3): 1959-1981.

[8]Liu B., Pavlou P. A. and Cheng X., Achieving a balance between privacy protection and data collection: A field experimental examination of a theory-driven information technology solution[J]. Information Systems Research, 2022. 33(1): 203-223.

[9]Monga V., Li Y. and Eldar Y. C., Algorithm unrolling: Interpretable, efficient deep learning for signal and image processing[J]. IEEE Signal Processing Magazine, 2021. 38(2): 18-44.

[10]夏义堃 and 管茜, 政府数据资产管理的内涵、要素框架与运行模式[J]. 电子政务, 2022(01): 2-13.

[11]曾铮 and 王磊, 数据要素市场基础性制度:突出问题与构建思路[J]. 宏观经济研究, 2021(03): 85-101.

[12]黄京磊, 李金璞 and 汤珂, 数据信托：可信的数据流通模式[J]. 大数据, 2023. 9(02): 67-78.

[13]包晓丽 and 杜万里, 数据可信交易体系的制度构建——基于场内交易视角[J]. 电子政务, 2023(06): 38-50.

[14]林镇阳, 侯智军, 赵蓉, et al., 数据要素生态系统视角下数据运营平台的服务类型与监管体系构建[J]. 电子政务, 2022(08): 89-99.

[15]范文仲, 完善数据要素基本制度 加快数据要素市场建设[J]. 中国金融, 2022(S1): 14-17.

[16]Rohn D., Bican P. M., Brem A., et al., Digital platform-based business models–An exploration of critical success factors[J]. Journal of Engineering and Technology Management, 2021. 60: 101625.

[17]窦悦, 易成岐, 黄倩倩, et al., 打造面向全国统一数据要素市场体系的国家数据要素流通共性基础设施平台——构建国家“数联网”根服务体系的技术路径与若干思考[J]. 数据分析与知识发现, 2022. 6(01): 2-12.

[18]王会金 and 刘国城, 大数据时代电子政务云安全审计策略构建研究[J]. 审计与经济研究, 2021. 36(04): 1-9.

[19]宋方青 and 邱子键, 数据要素市场治理法治化：主体、权属与路径[J]. 上海经济研究, 2022(04): 13-22.

[20]黄科满 and 杜小勇, 数据治理价值链模型与数据基础制度分析[J]. 大数据, 2022. 8(04): 3-16.

[21]Robinson S. L., Trust and breach of the psychological contract[J]. Administrative science quarterly, 1996: 574-599.

[22]Burt R. S. and Knez M., Kinds of third-party effects on trust[J]. Rationality and society, 1995. 7(3): 255-292.

[23]Mayer R. C., Davis J. H. and Schoorman F. D., An integrative model of organizational trust[J]. Academy of management review, 1995. 20(3): 709-734.

[24]周怡, 信任模式与市场经济秩序——制度主义的解释路径[J]. 社会科学, 2013(06): 58-69.

[25]Rousseau D. M., Sitkin S. B., Burt R. S., et al., Not so different after all: A cross-discipline view of trust[J]. Academy of management review, 1998. 23(3): 393-404.

[26]Zucker L. G., Production of trust: Institutional sources of economic structure, 1840–1920[J]. Research in organizational behavior, 1986.

[27]Luhmann N., Trust and power. 2018: John Wiley & Sons.

[28]Sako M., Price, quality and trust: Inter-firm relations in Britain and Japan. 1992: Cambridge University Press.

[29]Sztompka P., Trust: A sociological theory. 1999: Cambridge university press.

[30]Bohnet I. and Huck S., Repetition and reputation: Implications for trust and trustworthiness when institutions change[J]. American economic review, 2004. 94(2): 362-366.

[31]Gilson L., Trust and the development of health care as a social institution[J]. Social science & medicine, 2003. 56(7): 1453-1468.

[32]全国信息标准化技术委员会, 信息安全技术-数据交易服务安全要求. 2019, 中国标准出版社: 北京.

[33]Hutchings A. and Holt T. J., The online stolen data market: disruption and intervention approaches[J]. Global Crime, 2017. 18(1): 11-30.

[34]肖建华 and 柴芳墨, 论数据权利与交易规制[J]. 中国高校社会科学, 2019(01): 83-93+157-158.

[35]Agarwal A., Dahleh M. and Sarkar T. A marketplace for data: An algorithmic solution. in Proceedings of the 2019 ACM Conference on Economics and Computation. 2019.

[36]Li C., Li D. Y., Miklau G., et al., A theory of pricing private data[J]. ACM Transactions on Database Systems (TODS), 2014. 39(4): 1-28.

[37]刘小霞, 张嘉熙, 王申, et al., 基于多方计算技术的 数据交易机制研究[J]. Big Data Research (2096-0271), 2022. 8(3).

[38]Acquisti A., Taylor C. and Wagman L., The economics of privacy[J]. Journal of economic Literature, 2016. 54(2): 442-492.

[39]Balazinska M., Howe B. and Suciu D., Data markets in the cloud: An opportunity for the database community[J]. Proceedings of the VLDB Endowment, 2011. 4(12): 1482-1485.

[40]Kourid A. and Chikhi S., A comparative study of recent advances in big data for security and privacy[J]. Networking Communication and Data Knowledge Engineering: Volume 2, 2018: 249-259.

[41]Goel P., Patel R., Garg D., et al. A review on big data: privacy and security challenges. in 2021 3rd International Conference on Signal Processing and Communication (ICPSC). 2021. IEEE.

[42]Katzir Z. and Elovici Y., Quantifying the resilience of machine learning classifiers used for cyber security[J]. Expert Systems with Applications, 2018. 92: 419-429.

[43]Feldman M., Friedler S. A., Moeller J., et al. Certifying and removing disparate impact. in proceedings of the 21th ACM SIGKDD international conference on knowledge discovery and data mining. 2015.

[44]杜自然, 窦悦, 易成岐, et al., TID-MOP：面向数据交易所场景下的安全管控综合框架[J]. 数据分析与知识发现, 2022. 6(01): 13-21.

[45]Tan W., Li L., Zhou Z., et al., Blockchain-based distributed power transaction mechanism considering credit management[J]. Energy Reports, 2022. 8: 565-572.

[46]Gupta P., Dedeoglu V., Kanhere S. S., et al., TrailChain: Traceability of data ownership across blockchain-enabled multiple marketplaces[J]. Journal of Network and Computer Applications, 2022. 203: 103389.

[47]Dai W., Dai C., Choo K.-K. R., et al., SDTE: A secure blockchain-based data trading ecosystem[J]. IEEE Transactions on Information Forensics and Security, 2019. 15: 725-737.

[48]Zheng K., Zheng L. J., Gauthier J., et al., Blockchain technology for enterprise credit information sharing in supply chain finance[J]. Journal of Innovation & Knowledge, 2022. 7(4): 100256.

[49]Zhang J., Zhao Y., Wang J., et al., FedMEC: improving efficiency of differentially private federated learning via mobile edge computing[J]. Mobile Networks and Applications, 2020. 25(6): 2421-2433.

[50]郑婷一, 庞亮 and 靳小龙, 平台经济中的数据与算法安全[J]. 大数据, 2022. 8(04): 56-66.

[51]Kefeng F., Fei L., Haiyang Y., et al., A Blockchain - Based Flexible Data Auditing Scheme for the Cloud Service[J]. Chinese Journal of Electronics, 2021. 30(6): 1159-1166.