

可信数据空间建设:制度、技术与治理

敦 帅¹, 柳恒超²

(1. 中共上海市委党校(上海行政学院)领导科学教研部, 上海 200233;

2. 中共上海市委党校(上海行政学院)校刊编辑部, 上海 200233)

摘 要:可信数据空间作为实现数据要素市场化配置的基础设施,其建设关乎国家数字主权与产业竞争力。本研究基于可信数据空间概念、基础与功能和相关理论,构建了可信数据空间建设的“制度-技术-生态”三维模型,通过破解数据要素流通中的“信任-安全-价值”三元悖论,为复杂商业环境下的数据要素的“可信-可控-可用”提供系统性理论工具。研究发现:(1)可信数据空间建设需遵循制度、技术、治理三位一体的协同发展逻辑;(2)核心技术聚焦隐私安全与可信验证的双重突破;(3)治理逻辑层面需建立多元主体协同共治与风险免疫系统的混合框架;(4)可信数据空间的价值实现依赖于技术工具与制度规则的适配性迭代。可信数据空间的高质量发展需构建制度创新、技术攻关与治理试验协同推进的体系,一是要加快出台《数据产权登记管理办法》,二是要设立国家级数据空间技术实验室,三是要探索“监管沙盒”机制推动跨境数据试点。

关键词:可信数据空间;前提条件;核心技术;治理逻辑

中图分类号:D922.17

文献标识码:A

在全球经济从工业经济向数字经济加速转型的过程中,数据要素作为一种新型生产要素,已成为驱动数字经济发展的关键引擎。伴随数据要素被正式纳入全球20余个国家的生产要素统计体系,人类也正在经历一场静默的认知革命,即数据流动已取代石油管道,成为数字经济时代的核心动脉。然而,这一“数字原油”的开采与炼化却深陷于“塔西佗陷阱”。据IDC最新预测,2025年全球数据总量将突破175ZB,但企业间数据流通率却不足3.2%^[1],这种价值创造与信任缺失的剧烈冲突,正催生着数据要素市场化进程中的“数字巴别塔”。在技术维度,中心化存储架构与碎片化加密标准导致“信任成本指数级攀升”,据USENIX OSDI的基准测试显示,跨平台数据交换的远程认证耗时占比达59.7%^[2];在治理层面,欧盟《数据治理法案》与中国“数据二十条”的相继出台,虽确立了数据主权的法律框架,但具体操作中仍存在较多的合规性灰色地带;在经济领域,数据持有方普遍面临“开放则有价值流失风险、封闭则导致市场萎缩”的“霍布斯选择”悖论,这种囚徒困境直接造成我国数据交易市场年规模较小,数据要素市场化水平严重滞后^[3]。可见,破解

数据要素市场化中的信任壁垒与合规摩擦,是实现数据要素高效流通的基础性命题^[4]。

可信数据空间作为一种全新的数据流通利用基础设施,是构建全国一体化数据市场的重要载体,可信数据空间建设或将成为破解数据要素市场化配置中安全与流通矛盾的关键路径,为数字化转型提供“安全底座”与“流通枢纽”的双重支撑。可信数据空间建设能够通过技术融合重构数据生产关系,为跨组织、跨行业的数据要素高效配置提供制度保障与技术基础设施,从而实现数据主权治理范式的创新,最终实现数据价值的安全释放与数字经济高质量发展。然而,现有关于可信数据空间的研究仍处于起步阶段,整体上呈现场景分散化、理论碎片化的特征,尚未形成融合技术逻辑与制度创新的理论框架,难以有效指导复杂场景下的数据确权、流通激励与风险治理实践^[5-7]。因此,研究可信数据空间的概念与功能,系统性剖析可信数据空间构建的基础条件、技术架构与治理逻辑,对于规范数据互操作性与保障数据安全、明晰数据产权与交易定价、创新应用模式与推广可复制经验、构建多元主体协同创新生态,从而实现场景驱动的理论建构与跨域治理的

实践路径具有重要意义。

1 理论基础与研究框架

1.1 可信数据空间的概念、基础与功能

数据空间是数字时代新型数据协作的基础架构,其本质为多主体在保留数据控制权的前提下,通过标准化协议实现跨域数据调用的技术框架。其核心聚焦于建立数据主权可控的流通范式,不仅突破了传统中心化平台的数据垄断风险,而且可以为后续安全、可靠的增强技术预留接口。其特征在于网络拓扑的去中心化、接口规范的强标准化、权限管理的可扩展化。可信数据空间是在数据空间技术基底上构建的具备内生安全属性的价值交换网络,通过融合隐私计算、区块链与智能合约技术,形成数据要素流通的全周期可信保障体系。其在维持数据跨域协作框架的基础上,实现了数据可用性与安全性的动态平衡。其核心能力包含:基于数字指纹与分布式账本的确权溯源机制,建立数据权属的原子化映射;依托多模态隐私计算框架的密态计算能力,保障数据流通的零知识验证;通过智能合约驱动的动态审计追踪机制,实现操作行为的链式存证与穿透式监管;构建违约行为的自动化识别模型,运用博弈论算法建立激励相容的追责体系。

一方面,2024年,国家数据局印发《可信数据空间发展行动计划(2024-2028)》,明确了可信数据空间的五项基础,即关键标准体系构建、核心技术创新突破、基础设施服务优化、治理体制机制完善以及国际合作网络拓展。其中,标准体系聚焦数据主权界定与互操作协议研发,技术创新着力突破隐私计算与分布式账本等可信技术瓶颈,基础服务强化数据全生命周期管理能力,治理机制构建涵盖法律合规与风险防控的立体化监管体系,国际合作推动跨境数据流通规则的互认与协同。这五项基础工程可以推动可信数据空间形成从技术到制度、从区域到全球的闭环支撑架构。

另一方面,可信数据空间作为数字社会演进中的新型基础设施范式,其架构设计通过系统性功能组件体系的协同演化,构建起数据要素可信流通的内生安全机制与价值网络拓扑。基于“架构解构-功能映射-协同演化”三重分析框架,能够深入揭示该基础设施范式的技术实现路径与协同运作规律。从具体内容看,身份认证功能,基于多因子身份

验证机制实施主体资质审查,构建参与主体的合法性准入屏障;存证溯源功能,依托区块链技术固化全生命周期数据轨迹,形成抗抵赖性存证体系;资源管理功能,通过元数据标准化编目建立跨域资源检索协议,实现异构数据资产的可发现性;访问控制功能,采用动态访问控制策略与细粒度权限管理模型,实施数据操作行为的实时约束;隐私计算功能,基于联邦学习/安全多方计算框架,构建数据价值提取与隐私保护的协同机制;安全沙箱功能,部署虚拟化隔离环境与数据泄露防护机制,实现敏感信息的安全可控利用;合约执行功能,通过自动化协议执行引擎与共识驱动的权益分配机制,保障交易规则的不可篡改性;价值评估功能,建立多维数据资产评价指标体系,开发基于场景适应性的量化分析模型。从内在关系看,可信数据空间采用分层协同架构实现功能集成。一是信任基础层,依托身份认证与存证溯源功能构建身份核验与行为存证机制,通过访问控制与隐私计算功能实施动态安全防护,形成可信协作的底层保障体系。二是交互枢纽层,基于资源管理功能建立标准化资源检索框架,结合安全沙箱功能的受控实验环境,共同支撑数据要素的可验证流转与合规化操作。三是价值转化层,借助合约执行功能实现协议自动执行与权益分配,依托价值评估功能构建数据资产多维量化模型,完成数据要素到市场价值的转化闭环。通过层次化功能耦合机制,可信数据空间可以实现“可信验证-资源交互-价值创造”的全链路贯通。可信数据空间的概念体系如图1所示。

1.2 可信数据空间的相关理论

传统数据管理理论构建的数据治理框架为可信数据空间建设提供了基础方法论支撑。角色职责体系与全生命周期管理模型为可信环境下的数据权责划分奠定了逻辑基础,数据质量维度与元数据管理标准为跨域数据流通的语义对齐提供了理论依据,数据安全分类控制原则则构成了可信数据空间权限管理机制的设计原型^[8]。然而,该理论仍存在一定不足,导致其在应对跨组织数据流通的复杂性时呈现理论工具局限性。治理范式以组织内部为中心,缺乏多方协同场景下的动态博弈模型,难以支撑可信空间内数据主权与共享收益的精准平衡;技术耦合深度不足,未涵盖隐私计算、智能合约等新型可信技术体系与既有管理流程的融合路径;风险防控机制停留在静态防护层级,未能针对数据要素流通中

实时变化的信任衰减、合规漂移等动态风险建立量化评估模型。

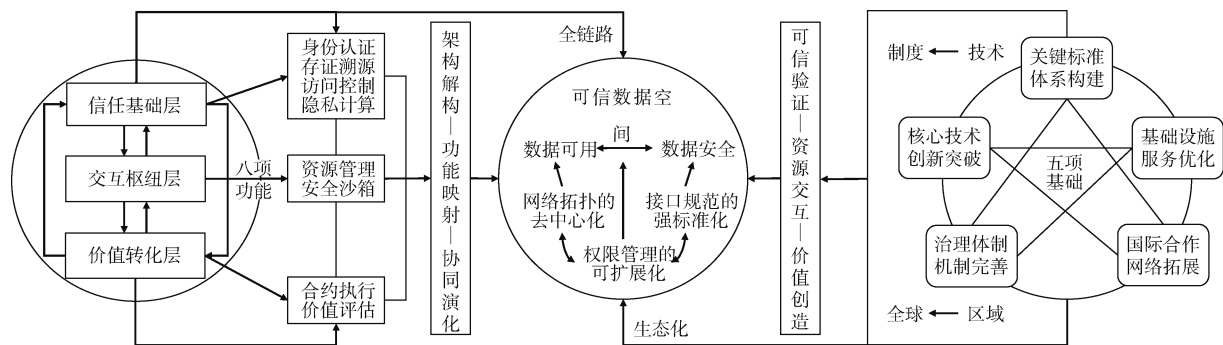


图 1 可信数据空间的概念体系

Figure 1 Conceptual system of trusted data space

数据要素化理论提出的“资源化—资产化—资本化”三阶模型,从经济学视角解构了数据要素价值转化路径,为可信空间内数据确权规则设计奠定了法理基础^[9]。其研究强调的数据资源持有权与数据加工使用权分离原则,直接指导了可信数据空间动态权限管理机制的设计逻辑;对数据非排他性、价值衍生性的特征分析,则为隐私计算与可信存证功能的技术架构优化提供了理论依据;研究构建的要素价值评估模型,通过引入边际成本递减规律,为可信数据空间价值转化层的市场化定价机制建立了分析框架^[10]。但是该理论在数据技术融合与动态治理层面的解释力存在不足。数据产权划分模型侧重静态权属配置,未充分考量多方协作中基于智能合约的动态权益协商需求,难以适配可信空间内实时权益调整场景;数据要素流通研究局限于传统市场机制,未深入融合数据沙箱、政府学习等新型可信技术对流通规则的改造效应;风险治理框架过度依赖制度约束,缺乏对数据流动拓扑网络的信任衰减建模,导致可信空间在应对多级供应链数据泄漏等复杂风险时缺乏量化评估工具。

可信数据空间理论通过多学科交叉融合,基于隐私计算与区块链技术,构建的“数据可用不可见”的流通范式,可以解决数据跨域协作中的信任难题,实现技术架构创新^[11];结合 DAMA 数据治理框架提出的动态权限管理模型,可以实现数据主权与共享价值的平衡与治理机制突破^[12];依托智能合约的收益分配机制,可以推动数据资产向资本转化,实现经济模型建构。该理论为可信数据空间建设提供了可扩展的“技术—制度”双轮驱动方案。但是,隐私计算的高算力消耗与法律合规要求尚未形成统一评

估标准导致技术与制度协同不足^[13],数据产权法律保障与技术实现路径存在断层导致理论与实践整合缺失^[14],供应链多级流转场景下的信任衰减量化模型缺乏导致动态风险建模滞后^[15]。这些缺陷导致理论在应对复杂商业生态时解释力受限。

1.3 可信数据空间建设的分析框架

基于以上分析,本研究尝试构建可信数据空间建设的“制度—技术—生态”三维模型,旨在通过规则约束、工具赋能与协作演化三者的动态协同,破解数据要素流通中的“信任—安全—价值”三元悖论。一方面,制度层聚焦数据权属界定与合规框架设计,为多方协作提供法律与规则保障;技术层以隐私计算、区块链等可信技术为核心,构建数据跨域流通的安全基座;生态层通过利益协调与场景适配,推动政府、市场与企业的价值共创。另一方面,制度可以约束技术应用的伦理边界,技术可以支撑生态协作的效率提升,生态可以实践反哺制度规则的迭代优化。三者有机融合突破了传统单一维度研究的局限,为复杂商业环境下的数据要素的“可信—可控—可用”提供了系统性理论工具。可信数据空间建设的分析框架见图 2。

2 可信数据空间建设的前提条件

可信数据空间作为数据要素市场化配置的核心载体,其建设需满足制度与技术双重前提条件。制度层面,需构建权责明晰的法律框架与合规体系;技术层面,需打造完善安全的基础设施与认证体系^[16]。通过制度与技术的协同演进,为可信数据空间建设提供规则约束与工具赋能双轮驱动的闭环

保障。

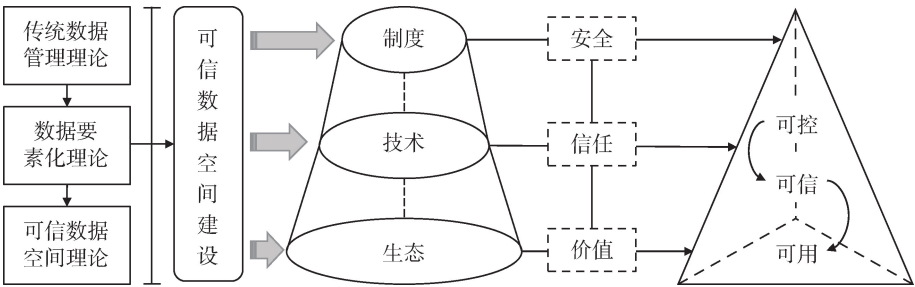


图 2 可信数据空间建设的分析框架

Figure 2 Analysis framework for trusted data space construction

2.1 制度前提

一方面,可信数据空间建设的制度前提始于数据权属立法的精准架构。首先,需建立数据权利主体的法定确权框架。面对个人、企业与公共机构间的数据权益冲突,立法应明确“三元权利结构”,即个人信息的自主控制权、企业数据的有限排他权及公共数据的开放使用权,通过权利边界划分解决主体间权责混淆问题^[17]。其次,需构建数据权属的客体分类体系。在数据要素非排他性特征下,传统物权法难以适配,需根据数据类型(原始数据/衍生数据)、流通场景(跨境/境内)实施差异化立法,限制其无序跨境转移,如德国《联邦数据战略》将工业数据纳入受限共享资产范畴^[18]。最后,需形成动态权属治理机制。借助区块链存证与智能合约技术,将法律条款转化为可执行代码,实现数据使用权流转的自动化追溯,如新加坡《个人数据保护法》对数据信托的法律定义^[19]。另一方面,可信数据空间建设的制度前提也源于标准体系构建的协同框架。其一,构建互操作性标准。针对异构系统间的数据接口与协议,需制定统一的技术互操作规范,破解跨平台协作中的“协议孤岛”问题,如 ISO/IEC 19941 数据空间参考架构^[20]。其二,完善数据分类与安全分级标准。基于数据类型和风险等级,细化流通权限与防护要求,如 NIST SP 800 - 60 对医疗数据的加密传输分级规则^[21]。其三,建立评估执行标准。通过第三方认证机构对数据流通全流程进行合规性审计,确保标准执行的可验证性,推动国际标准协同并建立标准与法律的衔接机制,实现从技术规范到制度约束的闭环治理。

2.2 技术前提

可信数据空间的技术前提需以新型数据基础设施架构为支撑,数据基础设施则以 5G 网络与算力

中心深度融合为基石。一方面,5G 网络可以为数据流通提供确定性的传输能力。基于 5G 技术的超可靠低时延通信 (URLLC) 可以保障工业物联网毫秒级时延要求,支撑实时数据交换^[22];而 5G 网络切片技术依托隔离、资源和优化的拓扑结构,可以确保不同垂直场景的数据传输安全^[23]。另一方面,算力中心可以构建弹性数据资源池。通过异构算力 (CPU/GPU/NPU) 池化与智能调度算法,可以满足隐私计算的算力密集型需求;依托“东数西算”国家枢纽节点,则可以优化跨地域算力负载均衡,降低数据传输能耗^[24]。同时,算网协同可以进一步推动数据架构创新。基于 SRv6 协议实现算力资源与 5G 网络的多维协同调度,实现数据的本地化处理^[25]。此外,分布式存储与计算架构、数据要素流通引擎及内生安全防护体系,可以推进新型数据基础设施的“零信任化”改造与数据编织技术融合,实现物理与数字空间的安全泛在互联^[26,27]。

3 可信数据空间建设的核心技术

可信数据空间建设的技术内核依赖于隐私增强技术与区块链存证技术的深度耦合。在隐私增强领域,需要突破密态数据可用性边界。一是基于全同态加密实现数据全生命周期加密态计算^[28],二是结合差分隐私动态注入噪声以平衡统计效用与个体隐私^[29],三是通过零知识证明构建最小化信息暴露的验证协议^[30]。在存证技术层面,需要构建多层级数据可信验证体系。一是基于改进型默克尔树实现高吞吐量操作日志压缩存储^[31],二是引入轻量化共识算法提升跨域存证效率^[32],三是通过链上预言机实现链外数据源的防篡改注入^[33]。两类技术的协同创新,不仅可以解决数据共享中的“隐私 - 效用”悖

论,而且能够通过不可抵赖的存证机制建立权属追溯的技术闭环。

3.1 隐私增强技术

可信数据空间的隐私保护体系需以多模态隐私增强技术协同架构为支撑。第一层级要聚焦数据可用性保障。通过安全多方计算构建分布式协同计算协议,使多方数据在密态下完成联合建模,避免原始数据外泄^[34];结合可信执行环境创建硬件级隔离的“计算飞地”,确保敏感数据在处理环节的物理防护。第二层级要强化动态隐私控制。引入基于场景自适应的匿名化技术,根据数据敏感度动态调整脱敏阈值,实现隐私强度与数据效用的弹性平衡^[35];同时利用合成数据生成技术,在保留统计特征的前提下替代原始敏感数据。第三层级要完善可验证机制。设计轻量化零知识证明协议,支持数据使用合规性的无信息泄露验证,满足多元高监管场景的审计需求^[36]。

3.2 区块链存证技术

可信数据空间的存证体系需依托区块链技术的多维度创新实现数据全流程可信锚定。第一,设计高并发存证数据结构。通过混合索引机制优化海量操作日志的存储与检索效率,支持工业场景下每秒万级事务的实时上链需求。第二,打造轻量化分层共识机制。采用分片技术与改进型实用拜占庭容错的协同架构,在保证去中心化特性的同时,将跨域存证延迟降低至亚秒级。第三,缔结可验证数据关联机制:基于智能合约构建动态数据血缘图谱,通过预言机与链下计算结合,实现链外数据源与链上存证的可验证映射。同时,要进一步探索可编辑区块链在合规擦除场景下的应用^[37],平衡不可篡改性 with 法律合规性要求,最终形成“存证-验证-治理”一体化的可信基础设施。

4 可信数据空间建设的治理逻辑

可信数据空间的治理架构需实现多元主体协同共治与动态风险防控的有机统一。在主体协同层面,需构建“政府监管-行业自治-企业自律”的三维治理框架。政府通过数据主权立法设定权责基准(如欧盟《数据法案》),行业协会建立跨域互操作标准(如国际数据空间联盟 IDSA 接口规范),企业联盟则设计数据贡献度量化模型(如通证化激励协议),形成规则制定、执行监督与利益协调的闭环。

风险防控维度需融合技术性阻断与制度性兜底。一方面,基于 AI 构建实时风险感知系统(如知识图谱驱动的异常行为检测),通过智能合约实施自动化合规拦截(如触发数据流权限熔断);另一方面,引入风险准备金制度与链上仲裁机制(如去中心化自治组织治理法庭),化解跨境数据争议与长尾风险。通过数字条约协商框架与可解释性 AI 技术协同破局,实现异构规则互认与算法黑箱破解。

4.1 治理主体协同

可信数据空间的治理效能依赖于多层级主体协同机制的创新设计。第一层级为国际组织与主权国家的规则协同。联合国国际贸易法委员会等机构推动跨境数据流通示范法制定,而主权国家通过数据本地化立法划定管辖边界,形成全球共识与主权保留的动态平衡。第二层级体现为跨行业联盟的技术标准协同。不同领域行业组织共建领域专用元数据模型,并通过互操作协议实现跨链数据交换。第三层级聚焦企业间的利益协同。基于区块链构建数据贡献度量化模型,依托智能合约自动执行收益分配,形成共建共治共享的激励闭环^[38]。同时,需通过主权间数字沙盒机制与链上治理的混合架构突破规则碎片化导致的合规成本激增(如不同国家数据分类标准差异达 47 项)及治理权责的灰度地带(如算法偏见归责主体模糊),打造技术标准嵌套法律规则的立体化协同范式,构建主体间权责可编程化映射的治理操作系统。

4.2 风险防控机制

可信数据空间的风险治理需构建预防-监测-处置一体化的动态防控体系。一是技术性风险阻断。基于联邦学习与边缘计算构建分布式风险感知网络,通过实时异常流量检测识别数据滥用行为,并依托可信执行环境实施敏感操作的硬件级隔离。二是聚焦制度性风险缓释。设计数据流通保险机制与链上风险准备金池,通过智能合约自动触发跨境数据泄露的赔付流程,同时建立链下仲裁庭与链上存证的协同裁决机制,实现争议解决的去中心化验证^[39]。三是强调动态适应性调整。利用强化学习算法构建风险策略自优化模型,根据历史攻击数据动态更新防控规则,并引入多方安全计算实现跨域风险情报的隐私保护式共享。四是通过主权间沙盒监管互认与量子抗性签名技术的融合,突破风险边界的模糊性及跨国司法管辖冲突,推进风险治理向代码化规则嵌套弹性容错的智能免疫系统演进。

5 可信数据空间建设的案例实践

可信数据空间通过技术创新与场景化应用,构建了数据要素安全流通与价值释放的双重能力。其核心实践围绕数据共享与垂域大模型两大方向展开:在数据共享领域,通过区块链确权、隐私计算与标准化数据共享接口,破解跨主体协作中的信任缺

失与隐私泄露问题,实现供应链协同、跨境合规、公共数据开放等场景的敏捷协作;在垂域大模型方向,基于可信环境融合多源数据,通过联邦学习、多模态融合与智能合约技术,开发行业级智能决策模型,提升不同实践领域的预测精度与运营效率。两类实践均强调“数据不出域”与“权责可追溯”,形成技术工具与治理规则协同驱动的数字化转型范式。可信数据空间的实践案例如表 1 所示。

表 1 可信数据空间的实践案例
Table 1 Practical cases of trusted data space

类别	案例名称	应用场景	技术方案	成效	场景价值
数据共享领域	工业制造供应链协同	供应链数据共享与敏捷制造(铁建重工、镭目科技)	区块链确权+隐私计算+动态 API 网关	采购成本降 3.43%,效率提升 13.2%	打破数据孤岛,支持质量追溯与敏捷制造
	跨境数据合规流通	跨境供应链数据传输(深圳数据交易所)	同态加密+API 网关+动态密钥管理	满足 GDPR 合规要求	化解主权争议与法律风险
	政府公共数据开放服务	户籍、教育、医疗数据开放(深圳市福田区)	数据脱敏工具+低代码平台	数据利用率提升 30%	赋能智慧城市决策与普惠服务
垂域大模型领域	新能源汽车电池风险模型	动力电池寿命预测与保险优化(中保协)	联邦学习+数据元件标准化	降赔减损率提升 23%,赔付成本降 3.9%	优化承保策略与风险预测精度
	大模型语料合规流通	语料数据场内交易(深数所、华为云)	可信数据空间+智能合约	数据滥用风险降低	解决训练数据确权与合规难题
	农业产业链智能决策	农产品价格预测(惠农网)	多源数据融合+农业知识图谱	农户收益提升 15%,库存周转率增 20%	优化供应链与提升农户收益
	气象灾害预警模型	台风路径预测(上海气象局)	多模态数据融合+可信训练环境	预测误差降 10%,应急响应缩短 30%	增强防灾决策能力与响应速度

注:API 指应用程序编程接口(Application Programming Interface);GDPR 指通用数据保护条例(General Data Protection Regulation),是欧盟 2018 年生效的一项数据保护法规,旨在加强个人数据安全与隐私保护。

6 结论与建议

可信数据空间作为实现数据要素市场化配置的基础设施,其建设关乎国家数字主权与产业竞争力。本研究基于可信数据空间概念、基础与功能和相关理论,构建了可信数据空间建设的“制度-技术-生态”三维模型,通过破解数据要素流通中的“信任-安全-价值”三元悖论,为复杂商业环境下的数据要素的“可信-可控-可用”提供系统性理论工具。研究发现,

(1)可信数据空建设需遵循制度、技术、治理三位一体的协同发展逻辑;制度前提上需构建主权立法与行业标准嵌套的规则体系,为跨域协作提供法律合规性保障;技术前提则依赖分布式架构、隐私增强技术与区块链存证的深度融合,形成可用不可见、

全程可追溯的技术闭环。(2)核心技术聚焦隐私安全与可信验证的双重突破:通过多模态隐私计算实现数据效用与隐私强度的动态平衡,依托可编辑区块链与零知识证明破解存证效率与隐私保护的矛盾。(3)治理逻辑层面需建立多元主体协同共治与风险免疫系统的混合框架:国际组织、主权国家与行业联盟需要通过数字条约沙盒实现规则互认,企业需要基于去中心化自治组织与通证激励模型形成自律生态,从而通过联邦风控网络与链上仲裁机制构建“预防-监测-处置”的全周期风险防控体系。(4)可信数据空间的价值实现依赖于技术工具与制度规则的适配性迭代。

可信数据空间的高质量发展需构建制度创新、技术攻关与治理试验协同推进的体系,以破解数据要素流通中权属模糊、技术掣肘与跨境壁垒三重难题。基于此,提出以下对策建议:

一是加快出台《数据产权登记管理办法》。数据产权登记制度是可信数据空间建设的法律基石,需要通过立法明确数据权属分置规则与登记流程。在立法框架上,可借鉴《民法典》物权编逻辑,构建数据所有权、用益权、担保权三级权利体系,明确数据所有者、加工者与使用者的权益边界。在登记机制上,依托国家级区块链平台构建分布式账本,支持数据指纹存证、权属变更链上追溯等功能,建立与市场监管总局企业信用系统的联动校验机制。在配套措施上,制定数据分类分级登记技术标准,设立数据产权交易备案中心规范数据流通合同范本,通过税收减免等政策激励企业主动登记。

二是设立国家级数据空间技术实验室。针对可信数据空间核心技术“卡脖子”问题,建议整合高校、科研院所与龙头企业资源,成立国家级实验室,如国家数据空间创新中心。研究方向上,聚焦隐私计算与区块链的协同架构优化,突破联邦学习模型收敛速度慢、跨链通信延迟高等瓶颈;研发自主可控的可信执行环境芯片;构建多模态数据流通仿真平台,测试跨境、跨行业场景下的技术适配性。运行机制上,可采取“揭榜挂帅”模式,设立开源社区推动技术成果转化,并联合 ISO/IEC JTC1/SC27 等国际组织参与标准制定。配套支持上,建立数据空间技术成熟度评估体系;开展“数据工匠”培养计划,培育复合型技术人才;设立跨境数据流动测试床,验证技术方案的全球兼容性。

三是探索“监管沙盒”机制推动跨境数据试点。针对跨境数据流动的规则冲突与监管不确定性,建议在自贸区开展“监管沙盒”试点。机制设计方面,一方面制定准入规则,限定试点企业数据合规能力和技术方案;另一方面开展动态评估,建立风险量化模型,实时监测数据泄露、主权争议等风险;同时推行容错退出,设置“创新豁免”条款,允许试错后无责退出。实施路径方面,优先选择 RCEP 成员国开展医疗、物流等场景试点;构建“白名单”互认机制,推动 APEC 跨境隐私规则与我国数据出境评估体系的衔接;建立沙盒数据保险池,由参与企业按数据价值比例缴纳风险准备金,需配套开发沙盒监管平台,实现规则代码化执行与风险自动化熔断。

参考文献:

- [1] IDC. Worldwide IDC Global DataSphere Forecast, 2024 – 2028: AI Everywhere, But Upsurge in Data Will Take Time[R]. Beijing, 2024.
- [2] Arnautov S, Trach B, Gregor F, et al. {SCONE}: Secure Linux Containers with Intel {SGX}[C]. 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16), 2016: 689 – 703.
- [3] 孟浩,王伟强. 数据要素驱动数字经济发展的现状、问题及应对建议[J]. 通信世界, 2024(12): 18 – 19. Meng H, Wang W Q. The current situation, problems and countermeasures of data – driven digital economy development[J]. Communications World, 2024(12): 18 – 19.
- [4] 包晓丽. 可信数据空间:技术与制度二元共治[J]. 浙江学刊, 2024(1): 89 – 100, 239 – 240. Bao X L. Trusted data space: Dual governance of technology and institutions[J]. Zhejiang Academic Journal, 2024(1): 89 – 100, 239 – 240.
- [5] 张妍,赵宇翔. 面向数据要素价值共创的可信数据空间培育思考[J/OL]. 图书馆建设, 1 – 7 [2025 – 03 – 27]. <http://kns.cnki.net/kcms/detail/23.1331.G2.20250324.1518.002.html>. Zhang Y, Zhao Y X. Reflections on the cultivation of trusted data spaces for the value co – creation of data elements[J/OL]. Library Development, 1 – 7 [2025 – 03 – 27]. <http://kns.cnki.net/kcms/detail/23.1331.G2.20250324.1518.002.html>.
- [6] 商希雪,冯洋,陆砚文. 城市可信数据空间中数据共享融合应用及其规范治理[J/OL]. 电子政务, 1 – 12 [2025 – 03 – 27]. <http://kns.cnki.net/kcms/detail/11.5181.TP.20250314.0924.006.html>. Shang X X, Feng Y, Lu Y W. Application and standardized governance of data sharing and fusion in urban trusted data space[J/OL]. E – Government, 1 – 12 [2025 – 03 – 27]. <http://kns.cnki.net/kcms/detail/11.5181.TP.20250314.0924.006.html>.
- [7] 樊振佳,刘亭孝. 可信数据空间:构筑文化数据流通与价值共创的新平台[J/OL]. 图书馆建设, 1 – 5 [2025 – 03 – 27]. <http://kns.cnki.net/kcms/detail/23.1331.G2.20250217.1547.004.html>. Fan Z J, Liu T X. Trusted data space: Building a new platform for cultural data circulation and value co creation[J/OL]. Library Development, 1 – 5 [2025 – 03 – 27]. <http://kns.cnki.net/kcms/detail/23.1331.G2.20250217.1547.004.html>.
- [8] Weymes E. A challenge to traditional management theory[J]. Foresight, 2004, 6(6): 338 – 348.
- [9] 梅宏. 数据要素化仍是国际性难题[N]. 中国科学报, 2022 – 09 – 01(1). Mei H. Data elementization re-

- mains an international challenge [N]. China Science Daily, 2022 - 09 - 01(1).
- [10] 陈刚, 颜斌斌, 汤珂. 数据的要素化与资产化: 理论辨析与实践探索[J]. 国际经济评论, 2024(5): 153 - 176, 8. Chen G, Yan B B, Tang K. Data elementization and assetization: Theoretical analysis and practical exploration [J]. International Economic Review, 2024 (5): 153 - 176, 8.
 - [11] 冯登国, 秦宇, 汪丹, 等. 可信计算技术研究[J]. 计算机研究与发展, 2011, 48(8): 1332 - 1349. Feng D G, Qin Y, Wang D, et al. Research on trusted computing technology[J]. Journal of Computer Research and Development, 2011, 48(8): 1332 - 1349.
 - [12] DAMA International. DAMA - DMBOK2: Data Management Body of Knowledge (2nd Edition) [M]. Technics Publications, 2017.
 - [13] 李建华, 银鹰, 李思源, 等. 大数据安全与隐私计算技术综述[J]. 网络空间安全科学学报, 2024, 2(6): 1 - 15. Li J H, Yin Y, Li S Y, et al. Review of big data security and privacy computing technologies[J]. Journal of Cybersecurity, 2024, 2(6): 1 - 15.
 - [14] 冯科. 数字经济时代数据生产要素化的经济分析[J]. 北京工商大学学报(社会科学版), 2022, 37(1): 1 - 12. Feng K. Economic analysis of data production factorization in the era of digital economy[J]. Journal of Beijing Technology and Business University (Social Sciences), 2022, 37(1): 1 - 12.
 - [15] GAIA - X Consortium. GAIA - X Architecture Document [EB/OL]. <https://gaia-x.eu/wp-content/uploads/2022/06/Gaia-x-Architecture-Document-22.04-Release.pdf>, 2022.
 - [16] Kairouz P, McMahan H B, Avent B et al. Advances and open problems in federated learning[J]. Foundations and Trends? in Machine Learning, 2021, 14(1 - 2): 1 - 210.
 - [17] Zech H. A legal framework for a data economy in the European digital single market: Rights to use data[J]. Journal of Intellectual Property Law & Practice, 2016, 11(6): 460 - 470.
 - [18] 毛一名, 青秀玲, 董瑜. 德国出台《联邦数据战略》, 增强数字主权 [EB/OL]. 科情智库 - 科技参考, https://mp.weixin.qq.com/s?__biz=MzI1MDI5ODkwMA==&mid=2247494622&idx=1&sn=ae55e5ad2297f8fccd00fa52e46b9c81&chksm=e986fca5def175b3d5bfc05468aa29a384550c88d0851cbb3fa59f47964bc77fdedf84aa6aa&scene=27. Mao Y M, Qing X L, Dong Y. Germany launches Federal Data Strategy to enhance digital sovereignty [EB/OL]. Science Intelligence Think Tank - Technology Reference, https://mp.weixin.qq.com/s?__biz=MzI1MDI5ODkwMA==&mid=2247494622&idx=1&sn=ae55e5ad2297f8fccd00fa52e46b9c81&chksm=e986fca5def175b3d5bfc05468aa29a384550c88d0851cbb3fa59f47964bc77fdedf84aa6aa&scene=27.
 - [19] 董春华. 新加坡《个人数据保护法》中的“数据携带”[N]. 中国社会科学报, 2021 - 06 - 07(2181). Dong C H. The term ‘data portability’ in Singapore’s Personal Data Protection Act [N]. China Social Sciences Daily, 2021 - 06 - 07(2181).
 - [20] ISO/IEC 19941. Information technology - Cloud computing - Interoperability and portability [S]. Vernier, Geneva, Switzerland: International Standard, 2017.
 - [21] NIST SP 800 - 60. Guide for Mapping Types of Information and Information Systems to Security Categories [S]. Gaithersburg, MD: U. S.: National Institute of Standards and Technology, 2008.
 - [22] 伏玉笋, 杨根科. 无线超可靠低时延通信: 关键设计分析与挑战[J]. 通信学报, 2020, 41(8): 187 - 203.
 - [23] 3GPP TS 28. 530. Management and orchestration; 5G end to end Key Performance Indicators (KPI) [EB/OL]. 3rd Generation Partnership Project (3GPP). https://www.3gpp.org/ftp/Specs/archive/28_series/28.530/.
 - [24] 中国信通院. 数据中心白皮书(2022年) [R]. 北京, 2022. China Academy of Information and Communications Technology. Data Center White Paper (2022) [R]. Beijing, 2022.
 - [25] 王晓云, 孙滔, 崔勇, 等. 算网协同: 构建新型信息基础设施和新型服务模式[J]. 信息与电子工程前沿(英文), 2024, 25(5): 629 - 634. Wang X Y, Sun T, Cui Y, et al. Coordination of networking and computing: Toward new information infrastructure and new services mode [J]. Frontiers of Information Technology & Electronic Engineering, 2024, 25(5): 629 - 634.
 - [26] 中国通信标准化协会, 中国信通院. 2024 零信任发展洞察报告 [R]. 广东, 2025. China Communications Standardization Association, China Academy of Information and Communications Technology. 2024 Zero Trust Development Insight Report [R]. Guangdong, 2025.
 - [27] 宋锴业. 数据编织、平台合作与生态联盟: 地方政府推动人工智能创新的机制研究——基于“国家人工智能创新应用先导区”的经验样本 [J/OL]. 电子政务, 1 - 13 [2025 - 04 - 02]. <http://kns.cnki.net/kcms/detail/11.5181.TP.20250314.0924.010.html>.

- Song K Y. Data weaving, platform cooperation, and ecological alliance: Mechanism research for local governments to promote artificial intelligence innovation – based on the experience sample of the “National Artificial Intelligence Innovation Application Pilot Zone” [J/OL]. E – Government, 1 – 13 [2025 – 04 – 02]. <http://kns.cnki.net/kcms/detail/11.5181.TP.20250314.0924.010.html>.
- [28] Gentry C. Fully Homomorphic Encryption Using Ideal Lattices[C]. Proceedings of the Forty – first Annual ACM Symposium on Theory of Computing, 2009: 169 – 178.
- [29] Dwork C, McSherry F, Nissim K et al. Calibrating Noise to Sensitivity in Private Data Analysis[C]. Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4 – 7, 2006. Proceedings 3. Springer Berlin Heidelberg, 2006: 265 – 284.
- [30] Tyagi S. A Review on Zero Knowledge Proof Vulnerabilities in Zcash[C]. 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICIT). IEEE, 2023: 872 – 877.
- [31] Gavin W. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014,151:1 – 32.
- [32] Luo D, Zhang Y, Sun G, et al. An efficient consensus algorithm for blockchain – based cross – domain authentication in bandwidth – constrained wide area IoT networks[J]. IEEE Internet of Things Journal, 2024,19(11):31917 – 31931.
- [33] Heiss J, Eberhardt J, Tai S. From Oracles to Trustworthy Data On – chaining Systems[C]. 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019: 496 – 503.
- [34] 汤凌韬,王迪,张鲁飞,等. 基于安全多方计算和差分隐私的联邦学习方案[J]. 计算机科学,2022,49(9):297 – 305. Tang L T, Wang D, Zhang L F, et al. Federated learning scheme based on secure multi – party computation and differential privacy[J]. Computer Science, 2022,49(9):297 – 305.
- [35] Sweeney L. k – anonymity: A model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge – based Systems, 2002, 10(5):557 – 570.
- [36] Ma L, Ge Y, Zhu Y. TinyZKP: A lightweight authentication scheme based on zero – knowledge proof for wireless body area networks[J]. Wireless Personal Communications, 2014,77:1077 – 1090.
- [37] 张驰骋,李雷孝,杜金泽,等. 可编辑区块链研究综述[J]. 计算机工程与应用,2024,60(18):32 – 49. Zhang C C, Li L X, Du J Z, et al. Redactable blockchain research reviews[J]. Computer Engineering and Applications, 2024,60(18):32 – 49.
- [38] Ronchi E, Reimsbach – Kounatze C. A Decade and A Half of OECD Action on Data Governance Policy – making[C]. Annales des Mines – Réalités industrielles. Institut Mines – Télécom, 2022(3):71 – 74.
- [39] Rusakova E P, Frolova E E. Digital disputes in the new legal reality[J]. RUDN Journal of Law, 2022,26(3):695 – 704.

Construction of trusted data space: Institutions, technologies, and governance

DUN Shuai¹, LIU Heng – chao²

(1. Leadership Science Teaching and Research Department of Shanghai Municipal Party School of the Communist Party of China (Shanghai Institute of Administration), Shanghai 200233, China; 2. School Journal Editing Department of Shanghai Municipal Party School of the Communist Party of China (Shanghai Institute of Administration), Shanghai 200233, China)

Abstract: As a new infrastructure for data circulation and utilization, trustworthy data space is an important carrier for building a national integrated data market. The construction of trustworthy data space may become a key path to solve the contradiction between security and circulation in the market – oriented configuration of data elements, providing dual support of “security base” and “circulation hub” for digital transformation. The construction of a trustworthy data space can reconstruct data production relationships through technological integration, providing institutional guarantees and technological infrastructure for efficient allocation of data elements across organizations and industries, thereby achieving innovation in the paradigm of data sovereignty governance, and ultimately realizing the secure release of data value and high – quality development of the digital economy.

Trusted data space is a value exchange network with endogenous security attributes built on the basis of data space technology. By

integrating privacy computing, blockchain, and smart contract technology, it forms a full cycle trusted guarantee system for the circulation of data elements. Its five foundations include the construction of key standard systems, breakthroughs in core technology innovation, optimization of infrastructure services, improvement of governance systems and mechanisms, and expansion of international cooperation networks. Its eight functions include identity authentication function, certificate traceability function, resource management function, access control function, privacy computing function, security sandbox function, contract execution function, and value evaluation function.

Based on the concept, foundation, function, and related theories of trusted data space, a three – dimensional model of “system technology ecology” for the construction of trusted data space has been constructed. By breaking the “trust security value” triple paradox in the flow of data elements, a systematic theoretical tool has been provided for the “trust controllability availability” of data elements in complex business environments. Research has found that: (1) The construction of trustworthy data space needs to follow the coordinated development logic of institutional, technological, and governance. Institutions can constrain the ethical boundaries of technological applications, technology can support the efficiency improvement of ecological collaboration, and ecology can practice feedback on the iterative optimization of institutional rules. The organic integration of the three has broken through the limitations of traditional single dimensional research and provided a systematic theoretical tool for the “trustworthiness controllability availability” of data elements in complex business environments; (2) The core technology focuses on the dual breakthrough of privacy security and trusted verification. The collaborative innovation of these two types of technologies can not only solve the “privacy utility” paradox in data sharing, but also establish a technical closed loop for ownership traceability through an undeniable proof mechanism; (3) At the level of governance logic, a hybrid framework of multi subject collaborative governance and risk immunity system needs to be established, and a three – dimensional governance model of “government regulation industry autonomy enterprise self – discipline” should be constructed to achieve the organic integration of technical barriers and institutional safeguards; (4) The realization of the value of a trustworthy data space depends on the iterative adaptation of technical tools and institutional rules.

The high – quality development of the trustworthy data space requires the construction of a system that promotes institutional innovation, technological breakthroughs, and governance experiments in a coordinated manner, in order to solve the triple problems of ownership ambiguity, technological constraints, and cross – border barriers in the circulation of data elements. Firstly, we need to accelerate the implementation of the “Measures for the Administration of Data Property Rights Registration” and clarify the rules and registration process for data ownership separation through legislation; Secondly, it is necessary to establish a national level data space technology laboratory to address the bottleneck problem of core technologies in trustworthy data space, integrate resources from universities, research institutes, and leading enterprises, and establish a national level laboratory; Thirdly, we need to explore the “regulatory sandbox” mechanism to promote cross – border data pilot projects. In response to the conflict of rules and regulatory uncertainty in cross – border data flow, it is recommended to carry out “regulatory sandbox” pilot projects in free trade zones.

Key words: trustworthy data space; prerequisite; core technology; governing logic