数字经济视角下数字信任体系的演进探析

文丨 王红叶 邵淼 黄莉群 梁钰林

随着数字经济向纵深发展，信任体系正经历从物理化、人格化向数字化、技术化的结构性变革。传统认证体系难以适应以万物互联和数据流动为特征的新环境。本研究剖析了数字信任在身份数据行为三个核心维度面临的系统性挑战，包括：第一，身份维度体现为主体边界从人扩展至智能体与设备；第二，数据维度体现为保护需求从静态存储转向动态流转与协同计算；第三，行为维度体现为责任界定从单一主体延伸至多方协同。在此基础上，本文提出应以密码学为基石构建多层协同的信任架构：通过增强型公钥基础设施与分布式身份技术，实现虚实身份的统一映射，借助同态加密与可信执行环境等技术，确保数据在可用不可见模式下的可信流通，并融合数字签名，构建可审计、防抵赖的行为存证链条。该框架为复杂的数字生态下实现可信交互提供了兼具理论连贯性与工程可操作性的路径参照，系统地构建了身份、数据及行为闭环联动的下一代数字信任基础设施。

数字经济视角下数字信任体系现状

数字经济的深化发展，正推动社会生产生活方式发生系统性变革。数字经济的崛起不仅重构了经济运行模式，更从根本上改变了“信任”的生成逻辑、承载载体及实现路径。在传统经济中，信任多建立于“熟人社会”的人际互动、实体凭证的物理背书（如纸质合同、公章）与线下场景的可感知性之上，具有“本地化、静态化、单一化”特征。而数字经济的虚拟性、跨域性、数据驱动性，推动信任形态从“人际信任”向“数字信任”跃迁，从“单一主体验证”向“全链条协同保障”升级，从“被动防御”向“主动赋能”转型。

信任缺失已成为制约数字经济健康发展的关键瓶颈。中国质量协会的《2020 中国数字经济服务质量满意度测评研究报告》指出，尽管 61.3% 的消费者对数字经济服务的交易安全性表示认可，但在数字经济相关法律法规的健全程度、隐私安全保护方面，多数受访者认为仍存在显著的提升空间。《2017 年全球互联网安全和信任报告》指出有 49%的受访用户表示，缺乏信任是不上网购物的主要原因，信任的缺失正在阻碍数字经济的进一步发展。两个报告共同印证：信任是数字经济健康发展的首要前提，构建规范化、可度量的数字信任体系已成为行业共识。

随着数字经济进入深化阶段，信任体系的载体升级与框架构建迎来了明确方向。国家数据局《可信数据空间发展行动计划（2024—2028 年）》明确提出，可信数据空间是支撑全国一体化数据市场的核心基础设施，需具备数据可信管控、资源交互、价值共创三类核心能力，且这三大能力本质对应“身份可信、数据可信、行为可信”的底层信任需求。数字化、智能化持续演进，车联网、物联网、云计算、AI 等新型基础设施快速发展，信任主体种类日益增加，已从个人、组织延伸到设备、应用、算法、AI 智能体等。网络实体和信任关系呈指数级、规模化增长，使得各类主体之间的跨域互信变得愈加困难，以 PKI 为代表的传统数字信任基础设施面临着全新的挑战。

数字信任体系变革面临的核心问题

大数据、云计算、区块链、人工智能等数字基础设施用于信息的采集、存储、分析及共享过程中，改变了信任的形式和信任建构的模式，传统的数字信任体系无法满足当前的安全需求。Gartner 将数字信任明确定义为“可衡量的信心”，其涵盖十个可信维度：身份唯一性、意愿表达、真实性、机密性、完整性、可用性、合规性、能力水平、可靠性、隐私性。这些维度并非孤立存在，最终也指向数字信任体系的三大核心要素，即“身份、数据、行为”。总之，“身份、数据、行为”三者共同构成数字信任的基础框架和主要的分析探究方向。

在“身份”方面，边界外扩冲击传统身份认证体系。传统身份认证依赖口令、智能 IC 卡、智能密码钥匙、动态口令令牌、生物特征等方式，在新技术场景下逐渐失效。一方面，以 AI 为核心的新应用生态中，延伸到设备、应用、智能体等，使信任边界外扩，其无法像人类一样记忆口令、具备可复制性且无生物特征标识，传统方式难以验证“虚体”完整性与来源真实性。另一方面，在万物互联背景下，终端节点数量庞大、设备种类丰富、通信模型复杂，现有身份与密钥管理机制无法适配多样化场景，急需设计场景化的身份管理和密钥管理机制，构建以密码技术为核心的物联网信任体系。

在“数据”维度，数据流转过程中存在隐私安全隐患。数据作为数字经济的核心资源，价值实现依赖于流通、加工、使用、交易等流转环节，然而这一过程会引发新的安全风险。传统的数据保护手段大多针对“静态数据”（如存储加密、传输加密），难以有效应对动态场景。在数据加工阶段，需防范隐私泄露；在数据交易阶段，需确保数据来源可信；在

（下转第 97 页）