

政务数据共享开放的安全技术路径与研究

王庆德

国家信息中心，北京，100045；

摘要：本文聚焦当前政务数据共享开放过程中面临的痛点难点问题，根据现存政府信息利用现状探求了一种新的政府数据开放共享模式，以解决目前政府信息开放共享模式中存在着跨部门间信息交流共享不充分和公民隐私信息实用性不达标核心难题，在技术可行性研究的基础上提出了基于区块链的政府大数据开放共享机制，阐述区块链技术在政务数据可信共享中的技术路径，更大程度地支撑和推动政府数据共享开放与创新应用，赋能数字中国建设。

关键词：政务数据；共享开放；安全技术

DOI：10.69979/3029-2700.25.08.023

1 政务数据共享开放现状分析

从国际上看，自 2009 年起，随着一系列诸如《透明和开放的政府》《开放政府令》等政策法规的出台，美国成为全球首个推广开放政府数据的国家，在全球范围内掀起了一波开放政府数据的浪潮。2013 年 6 月，法国、美国、英国、德国、日本、意大利、加拿大和俄罗斯八国集团首脑在北爱尔兰峰会上签署《开放数据宪章》，世界各国政务数据资源开放的呼声愈发高涨，各国、各地区将宪章作为开放数据的重要依据和原则，相继拉开了政府开放数据的大幕。为加强各部门所掌握的海量数据资产开放与共享，促进社会应用创新，美、英、澳、法等国政府均制定政府数据开放共享政策。各个国家在政府数据开放政策上具备两个共性特征：一是数据开放政策均建立在开放政府行动之下，使得数据开放有了更高的战略支撑；二是建立数据开放门户成为普遍趋势，有力保证政策得以落地。

从国内看，在国外积极推动数据开放的大背景下，2012 年上海公共数据开放网站作为全国首个公共数据开放平台向社会发布，之后陆续有北京、湛江、无锡等地也建设了自己的开放网站，在 2015 年出台《促进大数据发展行动纲要》以后，全国数据开放呈现爆发式增长，政务数据开放进入快车道。2017 年 5 月，国务院办公厅印发《政务信息系统整合共享实施方案》，提出建设“大平台、大数据、大系统”，形成覆盖全国、统筹利用、统一接入的数据共享大平台，分别依托电子政务内网、电子政务外网建设数据共享交换平台，构建多级互联的数据共享交换平台体系，促进重点领域信息向各级政府部门共享。

2 政务数据共享开放面临的问题

目前我国政府数据共享主要是基于数据交换共享中心的政府数据共享模式，各部门不再依靠个人或部门间的关系进行数据共享，而是接入本省或本市的大数据共享交换中心统一进行政府数据共享的模式。各级政府部门在推进政务数据共享开放的过程中，仍然存在着政府及公众对政务信息资源共享的需要与共享的不充分、不平衡之间的矛盾，其共享开放中突出问题主要体现在以下几个方面。

2.1 理念未达成共识，共享主动性不强

部分政府部门仍旧存在固有的工作模式和思维方式，私有化理念仍然存在，各部门对数据共享开放后的数据存储、数据安全、数据确权等权责问题的界定依然不够清晰，影响着政务数据共享开放工作的推进。

2.2 技术与标准不统一，共享渠道受阻

数据共享标准不统一主要体现在两个层面，一是系统层面。现有政务数据资源分布于不同政务系统中，各业务部门的政务系统基于各自业务需求而建，数据存储结构、技术标准不统一，系统之间无法兼容和对接，普遍存在各垂直业务系统之间、各垂直业务系统与大数据平台之间不能互连互通的问题，客观上造成了“数据孤岛”。二是数据层面。各部门沉淀的数据中，核心业务元数据标准不统一、业务数据串数名称、格式存在较大差异，对跨部门之间数据汇聚、共享、应用造成阻碍。

2.3 数据安全难以保障，共享风险高

网络信息技术促进了我国建设服务型政府的步伐，也带来了一定的风险。对于数据整合共享的安全防护措施和数据运维管理技术体系还未形成通用性的标准规范，缺乏统一的数据整合共享的信息安全顶层设计，各

部门系统网络安全等级保护标准不统一、防护等级不相同的现状普遍存在。数据可追溯性差、加密技术不完善、缺乏及时的评估指导和监督管理等方面,让政府部门之间不敢轻易的进行数据共享。

3 政务数据共享开放安全技术体系

3.1 数据应用安全关键技术

3.1.1 区块链技术

区块链技术本质上是一个分布式账本,通过其不可篡改、去中介化、可追溯等特点,让数据账本安全可信,有助于降低成本、增加协同和提高效率。一方面,能够打通政务“数据孤岛”。利用区块链数据存储方式,为链接链上的参与各方建立数据交易的信任基础,在政务数据共享过程中,实现数据确权、安全加密、多方安全计算技术,维护跨部门、跨地区、跨层级合作,优化政务服务,简化企业、群众办理业务的流程,增强政府公信力。另一方面,可以保证数据安全。区块链可建立非人为控制的信任系统,利用分布式节点共识算法来生成和更新数据,在区块链与政务深度融合过程中,打破数据归属权、管理权和使用权难界定的问题,实现各地区、各部分之间以信任和共识为基础的数据流通。

3.1.2 共识机制

区块链共识机制的目标是使所有的诚实节点保存一致的区块链视图,同时满足两个特性,一是一致性,即所有诚实节点保存的区块链的前缀部分完全相同;二是有效性,即由某诚实节点发布的信息终将被其他所有诚实节点记录在自己的区块链中。区块链的自信任主要体现于分布于区块链中的用户无须信任交易的另一方,也无须信任一个中心化的机构,只需要信任区块链协议下的软件系统即可实现交易。区块链技术正是运用一套基于共识的数学算法,在机器之间建立“信任”网络,从而通过技术背书而非中心化信用机构来进行全新的信用创造。

3.1.3 数字身份

区块链时代,先行者提出了数字身份的概念。试图用区块链来管理、保存、验证用户身份,同时支持自主选择部分身份属性开具称为“可验证声明”的电子证明,让用户对自己的身份有自主权。在传统方式中,用户的注册和身份管理完全依赖于单一中心的注册机构;随着区块链技术的出现,分布式多中心的身份注册、标识和管理成为可能。数字身份凭证的详细信息,出于对用户隐私的保护,通常为链下加密存储,存储在用户控制的存储区中,而将用户身份凭证的信息摘要到链上。

3.1.4 数据沙箱

数据沙箱是一款通过实现数据所有权和数据使用权分离,以确保数据流通过程安全可控的产品。数据沙箱具有完善的数据安全体系、完整的线上流程和灵活的算法实现模块等突出优点,在打破数据垄断,让数据流通便捷安全,实现数据民主化等方面发挥重要作用。

3.1.5 隐私计算

隐私计算本质上是在保护数据隐私的前提下,实现“数据可用不可见,非授权不可用,数据可控可计量”、“不共享数据,而是共享数据价值”等。隐私计算主要相关技术包括基于协议的安全多方计算;基于现代密码的联邦学习;基于硬件的可信执行环境。

3.1.6 数据脱敏技术

数据脱敏技术主要目标是按照脱敏规则通过变形、转换等方式降低数据的敏感程度,在数据的采集、传输、使用等环节中最小化敏感数据的暴露。在政务领域,由于政务信息来源于各政府部门的第一手数据,必然涉及大量个人信息。为保障政务平台安全,严防敏感数据泄露,政务领域中数据脱敏技术被应用于敏感数据采集、传输、使用等在内的全生命周期。

3.2 区块链在政务数据共享中的核心价值

区块链技术作为近年来最具潜力的技术之一,早在2016年12月就被作为战略性前沿技术纳入《“十三五”国家信息化规划》。2019年10月,习近平总书记在主持中央政治局集体学习时,针对区块链政务做出了细致部署,“探索利用区块链数据共享模式,实现政务数据跨部门、跨区域共同维护和利用,促进业务协同办理,深化‘最多跑一次’改革,为人民群众带来更好的政务服务体验。”

在理论上,区块链基于点对点的分布式记账技术、共识机制、非对称加密算法以及智能合约等多种技术,能够为参与各方建立强大的信任基础,链接链上各方,为链上各方的可信数据交互提供技术支撑。在政务信息化改革中引入区块链技术,能够实现政务数据的授权共享、业务协同,夯实智慧政府基础。

在实践上,区块链通过在各政府部门设立区块链节点,实现政务数据共享过程的数据确权、控制信息计算、个性化安全加密等。利用区块链的“去信任化”特性,打通政务数据孤岛,为原有部门条块化的数据授权共享与业务协同提供技术基础。

3.3 基于区块链技术的共享开放模式

针对政务数据共享开放中存在的诸多问题,提出了

基于区块链技术的共享开放新模式,保障政务数据共享开放的顺利推进,支撑国家治理能力和治理体系现代化建设。本文主要研究基于联盟链方式的国家政务数据共享开放模式。国家各部门构成区块链上的各个节点,借助已基本建成的国家政务外网,构建不同层级的(国家、省、市三级结构)区块链结构,每一级结构中可选择单个或多个节点作为“盟主”,管理区块链结构中的数据调用、日志变动等信息,当链上发生数据调用、记录交换时,“盟主”负责审核日志,并广播到整个区块链网络中,层级之间的数据调用、交换由各层级的“盟主”沟通获得。同时,政企之间可通过构建“共享沙箱”实现政务数据区块链网络与企业区块链网络的逻辑连接,达到“可用不可得”的目标,解决政企间的互信机制。

结合区块链的去中心化、去信任、集体维护、可靠数据库等主要特性,可以应对政务大数据基础库建设的难点。政务大数据的基础库包括人口库、法人库和电子证照库等,其数据来源是各个委办局,基于一数一源的原则,整合后的资源库可以服务于政务服务的数据查验和数据分析等。对于政务服务的支撑,关键是汇聚数据的准确、完整、安全、可追溯,通过区块链的去中心化特征,可以降低委办局上报数据的难度,通过区块链统一数据汇聚方式;去信任特征可以确保上链数据的安全及可验证,所有变化可追溯;集体维护和可靠数据库特征保证了数据存储的安全,以及数据的不可篡改,增加数据的权威性,也解决了委办局对于提供出去数据的安全担忧。

4 应用推广对策与建议

4.1 以区块链技术为基础支撑,构建一体化政务区块链平台

为政务数据共享交换与应用提供基于区块链可信环境。通过建设可信数据源管理机制确保数据来源安全,建设基于区块链的数字身份锁定数据责任主体,依托区块链不可篡改的特性,实现数据存证溯源能力;建设基于区块链的数据网关对数据范围进行认证、授权和审计,使数据流向可被全程追踪;建设基于区块链的数据铁笼,做到数据可用不可见、打造数据非授权不可用壁垒,解决内部数据使用过程管控问题。实现共享数据真实可信、实时流通、确权清晰、痕迹可查,进一步夯实城市大数据底座,助力政府数字化转型。

4.2 制定上链技术标准及规范,推动区块链平台规范应用

编制发布省级一体化政务区块链平台建设实施方案,指导全省政务区块链平台建设和政务数据上链与创新应用工作。在现有共享交换平台数据标准要求上,研究制定上链数据目录标准、数据上链标准、“跨链”标准和政务数据上链技术规范,实现数据上链和链上数据互联互通,确保标准统一。

4.3 推动政务数据上链,强化政务数据可信共享开放

依托共享交换平台在各业务数据系统实现的前置服务,通过提供标准 SDK 或相关接口,实现各业务数据系通接入“区块链网络”,支持各业务系统对自身数据自主管控的前提下,高效准确对外输出。实现将敏感核心数据进行链上存证,实现共享交换过程全程记录,支持数据流转溯源。以数据在平台的全生命周期流转过程为主线,经过数据资源库、主题库、数据共享、数据应用几个核心环节的行为基于区块链的审计,实现对数据的监控。完善数据采集及更新机制,制定相关数据业务标准,加强数据采集源头管理和数据治理,提升数据编目、整合、分析、展现、安全等管理和服务能力,全面开展数据质量管理,确保采集数据的准确性、完整性、时效性。

参考文献

- [1]王庆德,韩晓露,张贺.基于云的电子政务信息资源共享与安全保障体系及应用前景研究.2022年西湖论剑·网络安全大会——数字城市安全治理理论论文集
- [2]王庆德,吕欣,王慧钧,刘海洋,秦天雄.数据安全治理的行业实践研究[J].信息安全研究,2022,8(04):333-339
- [3]董超,王晓东,史田雨,王皓磊.基于区块链技术的政务数据共享开放模式研究[J].中国经贸导刊,2020,(8):4-5
- [4]李国良.提升数据共享安全能力的措施[J].中国信息化,2022(10):63-64

作者简介:王庆德(1982.08--),男,汉族,福建漳州人,高级工程师,博士,研究方向:电子政务、数字经济等