Doi:10.11835/j.issn.1008-5831.fx.2022.05.001

欢迎按以下格式引用:匡梅.主权区块链:政府数据开放的创新治理模式[J].重庆大学学报(社会科学版),2023(6):205-219.
Doi:10.11835/j.issn.1008-5831.fx.2022.05.001.

Citation Format: KUANG Mei. Sovereign blockchain: An innovative governance model of government data opening [J]. Journal of Chongqing University (Social Science Edition),2023(6):205-219. Doi:10.11835/ j.issn.1008-5831.fx.2022.05.001

主权区块链:政府数据开放的创新治理模式

匡 梅
(上海交通大学 凯原法学院,上海 200030)

摘要:现行政府数据开放的"集中—分布"模式既存在过度中心化的痼疾,又难以保障数据分布的整体效果。在数据集中的过程中,多节点数据难以汇聚至中心节点;在数据分布的过程中,中心节点数据难以传递至多节点;在数据利用的过程中,多节点与中心节点之间难以互动。鉴于此,需转变现行政府数据开放的模式,并为其寻求一种新的技术支撑。区块链是破解政府数据开放难题的理想技术,可以通过通信、存储、安全、共识等四层机制保障数据流通,克服单点故障和科层组织局限,并促使政府转变职能、赋能多元主体参与数据开放。但将单一区块链技术应用于政府数据开放时仍面临着规避监管、固化错误、破解算法和再中心化的危险,存在去中心化、安全性与可扩展性不可兼得的问题。面对政府数据开放的技术需求与区块链技术的三元悖论,本文通过引入主权区块链概念来探寻能够兼顾中心化的主权国家监管与去中心化的区块链技术的政府数据开放路径。主权区块链与政府数据开放存在契合之处,其本质是一种科技与制度叠加的、具有分布式整合功能的治理技术。依托于主权区块链,可以建构一个政府引导、节点共治的政府数据开放模式。具体而言,主权区块链由公有链、联盟链、私有链共同塑造而成,该构造有助于克服单一区块链技术的三元悖论。据此,在政府数据开放中,可以根据不同的数据类型、应用场景选择合适的区块链,通过搭建社会公众的公有链平台、推进协同机构的联盟链治理、筑牢职能部门的私有链隔离来塑造一个"以链治链"的主权区块链。在基于主权区块链的政府数据开放中,具有分布和开放特征的公有链有助于底层数据的互通与联盟链的接入。联盟链既可以通过将参与节点限定在有限范围内以构建政府部门间的数据共享平台,又能够通过嵌入公有链建立起"法链",将区块链置于主权框架下以保障国家监管。公有链上的数据将受到联盟链检验,其中敏感数据将保留在私有链上,其他数据则由公有链向外传输。私有链则用于为被分流的敏感数据提供安全的存储环境。

关键词:政府数据开放;区块链;主权区块链;法律治理;以链治链

中图分类号:D63 **文献标志码**:A **文章编号**:1008-5831(2023)06-0205-15

基金项目:上海市哲学社会科学规划青年课题"上海智慧城市建设中自动化决策的风险与问责研究"(2020EFX007)

作者简介:匡梅,上海交通大学凯原法学院,Email:kuangmei@sjtu.edu.cn。

一、问题的提出

当下,智能技术的发展日异月新,数据已成为一种重要的资源。政府在履职中收集、保留了大量数据,也因此成为了人类社会主要的数据持有者,但大部分政府数据仍被束之高阁。因此,为了释放政府数据价值,开放政府数据已成为各国政府亟待应对的时代课题。2015年8月31日,由国务院发布的《促进大数据发展行动纲要》(国发〔2015〕50号,以下简称《行动纲要》)中提出我国要建成统一的政府数据开放平台。但这种政府数据开放模式尚存在过度中心化的问题,故需探寻新的技术支撑和开放路径。近年来,一种分布式账本技术——区块链的应用范围逐渐从金融领域拓展至社会领域,并被认为是一种可以破解政府数据开放等政务难题的理想技术。于是,各国相继将区块链运用于具体的政务实践场景。习近平总书记亦强调:"要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。"①简言之,区块链在透明、高效、安全地开放政府数据时具有极大潜力。

但问题在于,在现行政府数据开放中,政府始终扮演着中心数据控制者的角色,而区块链的创设初衷在于脱离政府监管束缚,从而建立起独立于主权国家的分权共治组织。因此,这种去中心化的区块链所代表的算法共识不可避免会对国家主权以及依托于国家主权的政府数据开放系统产生冲击。然而,随着大数据时代的到来,将区块链和政府建设相结合已是大势所趋,这是一场"中心化"与"去中心化"相向的运动。那么,如何将区块链运用于政府数据开放?如何处理好去中心化的区块链技术和中心化的政府数据开放之间的关系?针对此问题,本文将剖析我国现行政府数据开放单中心模式的局限之处,并分析区块链的技术特征及其在政府数据开放中的应用前景与监管难点,最终探寻一条能够兼顾区块链技术与国家主权的政府数据开放路径。

二、中心权威:政府数据开放的现行模式及困境

(一)政府数据开放的"集中—分布"模式

20世纪50年代,国际上兴起了政府信息公开运动[1],其侧重点在于对政府信息的公开和对公众知情权的保障。智能科技的蓬勃发展推动人类社会从IT(Information Technology)时代迈向DT(Data Technology)时代。在此过程中,二进制样态的数据发挥着承载信息的作用。作为社会事务的管理者,政府在履职中积累了大量数据。数据是可以被利用的宝贵资源,但唯有通过自由流通才会产生价值。在此背景下,开放政府数据(Open Government Data)就成为建设智慧型政府、推动经济可持续发展的重要支撑,这也是政府信息公开在当代的新发展。为了加速开放数据的传播和再利用,世界各地的许多政府已经公开了它们的数据[2]。我国亦高度重视政府数据开放,颁布了《中华人民共和国数据安全法》《政务信息系统整合共享实施方案》《提升全民数字素养与技能行动纲要》等一系列法律法规、政策文件,各地方政府也在加快推进政府数据的开放。

目前,学界对"政府数据"的定义较为统一,陈尚龙[3]、沈亚平[4]等大多数学者都将其界定为行政机关(包括被授权行使行政职权的机构)在履行职能时采集、产生和保存的数据。就"政府数据开

①央视网:《习近平在中央政治局第十八次集体学习时强调 把区块链作为核心技术自主创新重要突破口 加快推动区块链技术和产业创新发展》,网址:http://news.cctv.com/2019/10/25/ARTIWOIBvCCUykO9uyfui42j191025.shtml,最后访问:2023年10月9日。

放”而言,学者则分别基于各自的立场对其进行了定义,主要形成了两种范式:一种范式侧重于凸显数据安全的关键性;另一种则强调数据流通的价值。例如,岳丽欣[5]、杨瑞仙[6]等学者在对政府数据开放进行定义时,着重强调不予开放政府数据的情形,即将侵犯个人隐私、危及国家安全的敏感数据排除在政府数据开放的范围之外。郑磊[7]、吴旻[8]等学者则从公众自由使用数据的角度对政府数据开放作了界定,强调开放数据是为个人提供自由使用的资源。上述两种范式体现了“安全话语”与“开放话语”之间的分歧,双方各执一词,难分胜负。因此,对政府数据开放的界定须回归到具体过程,其可被分解为两层含义(见图 1)。

图 1　政府数据开放的“集中—分布”模式

第一,政府数据开放蕴含着“集中”之意。现代政府建立在科层制基础之上,这一自上而下的管理模式强调政府的一元主体地位。奉行科层制的政府按照“金字塔”式的等级结构确立、巩固权威,并逐步塑造了一个权力中心。也就是说,科层结构强化了政府在社会中的权力中心地位。我国政府采用的正是科层组织结构。政府数据开放也被整合到科层体制中,成为一种组织化的传播工具,因而会受到行政机关(或被授权行使行政职权的机构)等中心数据控制者的影响。当前,构建统一的数据开放平台是推进政府数据开放的主要方式。我国北京、上海、深圳等地已陆续建立起政府数据开放平台(例如,上海市公共数据开放平台)。负责该平台运作的政府部门需具有数据采集、处理、存储等方面的能力。数据采集能力是指政府数据开放平台从政府各部门或公众采集数据,并将分散的数据汇聚成一个个数据集(Data Set)时需具备的能力;数据处理能力是指政府数据开放平台对被采集的数据进行清洗(Clean)、脱敏(Mask)、维护(Maintain)等时需具备的能力;数据存储能力是指政府数据开放平台对经过处理的数据进行存储时需具备的能力。在此过程中,政府自上而下推进并介入数据集中的各个环节,采用单向度的方式将原本分散于各部门、各领域且互不兼容的数据整合到中心数据库。这种单向、封闭的模式体现了政府本位、内部程序导向的科层理念。

第二,政府数据开放蕴含着“分布”之意。虽然政府数据开放呈现出了中心化趋势,但互联网本身具有扁平化特征,加之政府数据开放强调数据被自由利用所可能产生的价值。因此,政府既要向公众输出数据,还要保障数据的再利用。如图 1 所示,数据从作为中心节点的政府数据开放平台向四周辐射。透明度和参与度是开放政府的重要评价标准。透明度是指政府信息向公民公开的程度;参与度涉及公民的参与和政府的响应[9]。因此,数据分布环节的重心在于保障数据的透明度和公众的参与度,这与政府数据开放平台的数据、接口、应用、互动等功能息息相关[10]。其中,数据功能是指平台通过数据分类、检索结果排序、数据开放格式提供、元数据描述等方式为用户浏览、检索、下载、使用数据提供指引;接口功能是指平台设置应用程序编程接口(Application Programming Interface,简称 API)以供用户快速获取数据;应用功能既包括平台开发应用(Application,简称 APP)以供用户下载、使用的情形,还包括用户利用公开的政府数据开发 APP,并将 APP 上传至平台以供其他用户下载、使用的情形;互动功能是指平台为用户提供数据申请、评分、分享等渠道,并向用户

征集APP、建议等。

(二)单中心政府数据开放模式的双重困境

表面上,政府数据开放呈现出了去中心化样态;实际上,政府是一个中心化的权力系统,其规定着去中心化的程度。在此情形下,数据被"冻结"在由政府创建的中心服务器中,随后自上而下向社会弥散。这种单中心政府数据开放模式既难以避免过度中心化的痼疾,又难以保障数据分布的整体效果。

首先,在数据集中的过程中,多节点数据难以汇聚至中心节点。一方面,科层组织内部跨层级、跨部门的数据整合难。政府数据共享是数据开放的前提。在科层体制中,政府内部"只能通过制度化组织渠道进行沟通"[11]。从纵向看,在金字塔式的组织结构中,层级链条过长,数据容易在上下级政府间的传递中失真。从横向看,同级政府部门间尚存在由于制度壁垒而"不能共享"和由于缺乏动力而"不愿共享"的情形。目前,我国各地方政府的数据开放大多由信息化主管单位(例如,经济和信息化委员会)统筹、管理,该主管单位的行政级别通常与其他具有数据处理职能的政府部门相同[7]。但问题在于,各政府部门大多关注与本部门相关的数据收集、发布,如果部门间缺乏数据交流机制,抑或权责分配标准不明确,将大大降低政府部门数据共享的积极性。另一方面,科层组织内部和外部的数据整合难。单中心政府数据开放模式符合信息传播范围有限的社会样态。但在大数据时代,智能技术的普及使每个个体同时身处现实的物理空间和虚拟的网络世界,面临着数据的"大爆炸"。在此背景下,单一、垂直的单中心政府数据开放模式在收集海量、分散的数据时,会面临数据超载、阻塞的问题。

其次,在数据分布的过程中,中心节点数据难以传递至多节点。一是中心系统是易受攻击的单一节点。阿特佐伊将层级组织中的集中权限用计算机术语定义为单点故障(Single Point of Failure,简称SPOF),他认为如果该节点发生故障,那么整个系统都将受到负面影响[12]。目前,我国政府数据开放始终无法脱离处于中心位置的政府数据开放平台的控制。由于该中心服务器公信力高、影响力大,如果发生数据泄漏或黑客攻击,那将是灾难性的[13]。二是中心系统无法对数据流进行全程监管。在现行数据开放模式中,即使单个数据集不涉及个人隐私,多个数据集的组合也可能会识别出个人信息。数据的融合会被用来勾勒公民的"完整档案"。但由于无边无垠的数据流没有时间标识和加密措施,中心系统无法对其进行全程追溯、保障,这会增加数据被篡改或泄露的风险。三是中心系统受制于科层组织的局限。在现行数据开放模式中,中心系统需支付平台维护成本,不断提高数据供给能力。但当潜在获益和维护责任不匹配时,相关部门会缺乏动力去推进数据开放。并且在科层体制内,中心系统所做的决策需层层向上请示,这可能会带来数据发布、更新的延迟,导致数据开放效率欠佳。例如,我国政府数据开放平台上的数据集大多是不可机读的PDF文件,而且数据通常未能得到及时更新,接口开放率也整体偏低,不少平台甚至尚未提供数据接口[10]。

最后,在数据利用的过程中,多节点与中心节点之间难以互动。开放数据旨在推动产生一个开放的政府。因此,政府不仅应向公众公布数据,还应鼓励公众提供反馈。目前,我国各地政府数据开放平台都在积极创建政府与用户之间的对话机制,主要通过向用户提供对数据集的请求、下载、评价、分享等渠道来实现。就数据请求而言,我国大多数政府数据开放平台均允许用户请求开放所需数据,但通常未能及时对数据请求作出回应。就数据下载、评价而言,我国大多数政府数据开放平台都需要用户提前注册或登录系统,但注册、登录等复杂操作不利于用户快速获取数据。并且大

多数政府数据开放平台都将用户的反馈建议封闭在后台,不予公开。就数据分享而言,仅青岛市人民政府数据开放平台向用户提供了将数据分享至其他社交平台的渠道[14]。分享功能的缺乏会阻碍政府数据开放平台的推广。可见,单中心政府数据开放模式难以回应多元节点的数据需求,这会阻碍用户自下而上地参与和监督。鉴于此,我们需要探寻一种能够促进多元节点之间合作和数据资源有效配置的替代方案。

三、分权共治:基于区块链技术的政府数据开放

(一)区块链在政府数据开放中的应用前景

1. 区块链的技术架构及其特征

中本聪在《比特币:一种点对点的电子现金系统》中介绍了不依托于国家主权的数字货币——比特币。虽然他在原文没有提到区块链这一术语,但比特币使用一系列被链接在一起的带时间戳的数据块的方式被认为是区块链现象的根源[15]。作为比特币的核心技术,区块链的诞生是为了应对金融危机后席卷全球的信任危机,试图在不可信的环境中创建可信的服务。

区块链技术一直备受关注,也引发了不少争议。由于理解侧重点的不同,学者们尚未对其形成统一定义。但大体而言,可以将其划分为狭义和广义两种界定方式。狭义的界定方式侧重于从核心特征出发来定义区块链。其中一种狭义的界定方式将区块链理解为"区块"与"链"(时间序列)的结合,重在突出区块链不可篡改、不可伪造的特征。例如,何蒲[16]、韩璇[17]等学者基于组织结构和运行原理将区块链理解为一种前后相连的电子账簿,其中每一个区块是账簿的一页,从第一页"链接"到最新一页。另外一种狭义的界定认为区块链是分布式数据存储方式,重在强调区块链的去中心化特征。例如,程啸[18]、石超[19]等学者将区块链视为一种分布式数据库解决方案,它维护不断增长的数据记录。

在广义层面上,学者基于综合视角对区块链作了界定,认为区块链组合了不同技术的优点,是一种综合性的信息技术。其中较为经典的是《块数据 3.0:秩序互联网与主权区块链》一书从广义层面对区块链的界定。该书以区块链中数据传递各环节所依凭的核心技术为出发点,将其界定为一种经由块链式数据结构验证和保存数据、经由分布式节点共识算法生成和更新数据、通过密码学方式保障数据传输和访问的安全、利用智能合约编程和操作数据的分布式基础架构和计算范式[20]39-40。此外,武岳[21]、蔡晓晴[22]等学者也从广义层面对区块链进行过界定。可见,为了更全面地认识区块链,我们需要对其技术架构和特征进行综合考察。区块链是对点对点传输、分布式数据存储、加密算法、共识机制等计算机技术的整合[20]39。如表 1 所示,可以将区块链的主要技术架构归结为通信、存储、安全、共识等四层机制。

表 1　区块链的技术架构

主要技术				其他
共识机制	工作量证明机制(PoW)	权益证明机制(PoS)	股份授权证明机制(DPoS)	
安全机制	非对称加密算法		哈希算法	.
存储机制	块链式数据结构			
通信机制	P2P			

处于区块链第一层的是"通信机制"。P2P(Peer-to-Peer,简称 P2P)网络是区块链的基础架

构[20]62。在P2P网络中,每个节点可以通过多播(即一点对多点的通信方式)实现路由、发现新节点以及验证、传播数据[23]。如图2所示,区块链中各节点同时扮演着服务器和客户端的角色,最终形成一个不依赖于中心服务器的分布式系统(Decentralized Systems)。基于分布式系统,区块链可以构建去中心化的服务,该服务能够与可信任的中心化服务实现相同的目标。

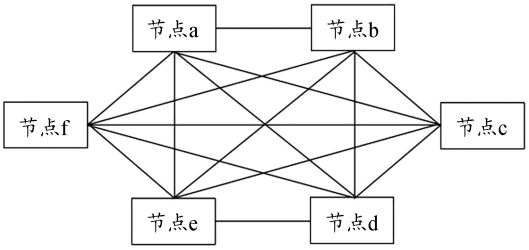

图2 P2P网络模式[24]

处于区块链第二层的是“存储机制”。经由P2P网络传播的数据以块链式数据结构存储在区块链上。所谓块链式数据结构,是指区块链中的数据以区块方式保存,然后以时间序列连接成“链”。区块由区块头(Header)和区块体(Body)组成[25]。其中区块体用于存储区块创设中生成的、经过验证的交易数据,区块头则负责与前一区块相连,同时以时间戳维系历史数据的完整性。据此,每个节点记录的数据都会被分享至整个区块链,并且所有节点都可以获取一份完备的数据副本。

处于区块链第三层的是“安全机制”。区块链的加密算法等安全机制可用于对数据进行保护,以防止数据被篡改或窃取。其中常用的加密算法包括非对称加密算法和哈希算法。非对称加密算法通过由公钥、私钥组成的密钥对数据进行加密、解密。在该算法的运算中,公钥对外公布,并对将要发送的数据进行加密,私钥则用于解密接收到的加密数据。并且,该算法可以保证从公钥无法反推出私钥。哈希算法则负责将输入的数据换算为具有固定长度的二进制值(也称为散列值或哈希值)。因此,区块链上每个数据的哈希值都是唯一的,据此可以检验数据的真实性。

处于区块链第四层的是“共识机制”。在区块链中,分布式节点在功能上就好像只有一个中心节点。各节点就规则达成一致离不开共识机制的保障。共识机制是区块链实现分布式自治的基础和前提,主要包括工作量证明机制(Proof of Work,简称PoW)、权益证明机制(Proof of Stake,简称PoS)、股份授权证明机制(Delegated Proof of Stake,简称DPoS)等[26]。中本聪提出的共识机制是PoW,它的本质是算力决定权力,付出最大计算工作量的节点将取得创造下一个区块的权力[27]。此外,区块链中各节点共识的达成还依托于可编程的智能合约,该合约在满足条件时自动执行。

2. 区块链对政府数据开放单中心困境的破解

虽然区块链设立的初衷是为比特币提供底层技术支持,但在可预见的未来,区块链将在社会生活的各个领域被广泛运用。其中,区块链和政务建设相结合已是大势所趋。尽管问题和担忧依然存在,但区块链确实改变了政府处理数据的方式,在破解政府数据开放中存在的单中心困境时,其呈现出了极大的应用前景。

在现行政府数据开放中,数据的集中离不开中心节点。但该模式难以整合不同政府层级、部门以及政府和公众之间的海量异构数据。区块链开创了去中心化的新时代,在这个时代,人们逐渐从信任人类代理人转移到了对开源代码的信任,这是一种基于共同协商、维护的算法式信任。区块链中的每个节点都运行一个共识算法,该算法提供了节点间就给定交易达成一致的方法,从而无需任

何人工干预,这可以降低个体机会主义风险,也能够加深各节点间的信任。并且,所有参与节点都持有区块链的副本,因此它们有权验证每次记录是否有效、合法。这些节点拥有相同的权力,都可以通过 P2P 网络发布、传输数据,而无主从之分。该模式既有利于推动数据在政府与公众之间的跨领域流通,又有助于在政府内部构建一个扁平的组织结构,保障政府数据共享。

在现行政府数据开放中,数据从中心节点分布至多节点。但该模式存在中心节点的故障通过多节点危及整个数据开放系统的风险。针对此问题,以区块链为支撑的政府数据开放的优势表现为如下三方面:一是独立节点。区块链中的数据可以以分布式方式存储,从而无需依托于可能导致单点故障的中心平台。二是多重备份。区块链上的数据具有块链式结构,所有节点都持有一份区块链的数据副本,并能够根据商定的规则去记录、跟踪数据操作的全过程。因此,即便某个区块的数据受到了攻击,该区块的多个副本还会继续存在。三是 51%攻击。在区块链中,任意节点数据的改动都会引起相应哈希值的变动,但只有在超过半数的节点被改动时,整个区块链的数据才会随之变化。然而,当前技术尚难以掌控区块链系统 51%以上的节点。

在现行政府数据开放中,数据由中心节点收集、发布和监管,故不可避免会受到中心系统科层体制的影响,从而面临着数据质量差、更新慢、监管难等困境。区块链在解决此问题时具备如下三方面优势:一是数据真实。在区块链中,区块的生成离不开全体参与者的共识,经由节点认可,数据方能输入区块链,并由所有参与者集体维护,节点之间可以相互监督。二是数据高效。区块链是可编程系统,各参与方可以通过智能合约来设计自动执行的合约关系。在此情形下,虽然没有强有力的监督中心,但仍能通过共识机制促使各节点遵循统一的协议,这样的自组织网络能够减少单中心模式收集、发布、监管数据的成本耗费,以及集中决策的时间耗费[28]。三是数据安全。在区块链中,经由非对称加密算法,数据受到了私钥、公钥的约束[29],每个私钥只能用于解密对应公钥加密的数据,从而保证数据不被非法读取。经由哈希算法,前一区块中任何数据的变动都会得出不同的哈希值,这可以确保数据不被非法篡改、操纵。并且,转换为二进制的数据无法直接与个人身份相联系,这可以保障数据的匿名性。经由时间戳,区块链上的数据流拥有了能够被追溯的时间标识。

在现行政府数据开放中,封闭的单中心系统会阻碍用户自下而上的数据下载、评价、请求和分享。区块链能够在技术层面保障政府数据开放中政府与用户之间的互动,具体表现为如下两方面:一方面,促使政府转变职能。区块链是一个分布式共识网络,其中所有交易都要向公众公布,具有公开透明的特征。在以区块链为基础的数据开放中,政府不再居于中心位置,而是与其他节点处于平等的地位。区块链促使政府不再要求用户去适应统一的标准,而是根据用户需求提供个性化服务。另一方面,赋能多元主体参与数据开放。区块链的出现可以被看作是公众参与权威的一种方式。区块链在最基本的层面上是开源代码,其底层协议和算法模型可被所有节点自由使用,并且各节点能够经由开放的接口读取、下载系统中的数据。基于此,各主体能够主动参与数据开放,而非被动的旁观者或接受者;各主体的诉求能够在点对点的分布式传输中得到及时反馈,这有助于在节点间形成“环环相扣”的“最长链共识”。

(二)区块链应用于政府数据开放的三元悖论

区块链可以赋能多元主体,提升政府数据开放的效率和质量。因此,许多区块链倡导者声称,可以用基于区块链的分布式开源平台取代国家的传统职能,将社会更有效地组织起来。这些“密码朋克”呼吁要用数理方式解决社会问题,致力于在区块链中实现“代码即法律”[30]6 的自治,打造一

个不受主权国家控制的自治社区。但在政府数据开放中采用单一的区块链技术尚存在如下危险。

区块链的通信机制存在规避监管的危险。虽然以区块链为支撑的政府数据开放能够为分布中的数据流提供监管技术,但当政府"嵌入"到P2P网络中后,就成为了众多节点之一,与区块链中的其他节点共同承担着监管责任。这就改变了现行数据开放中政府主导的局面,政府权力也面临着私主体化的危险,不得不让渡部分权力。在此情形下,若节点之间未就数据传播等事宜订立智能合约,抑或缺乏法律层面的监管措施,区块链的运用极易面临相互推责而又无人担责的困境。例如,有学者认为,在责任认定方面,区块链"缺乏必要的中心机构为其运作承担监管义务与法律责任"[31]。

区块链的存储机制存在固化错误的危险。在区块链中,块链式数据结构和哈希算法增加了攻击者对单个区块数据修改的难度,保障了数据的不可篡改性。就智能合约而言,由于区块链的所有交易都包含在了哈希链中,因此是不可更改的,但合约中的错误或缺陷会给系统带来风险。就数据存储而言,在块链式数据结构中,原本存在错误或隐私泄漏风险的数据同样难以被修改或删除,这会固化区块链中的错误数据。

区块链的加密机制存在算法被解密的危险。在非对称加密算法中,攻击者可以通过破解区块链中某个节点的私钥以读取该节点数据,并通过聚类算法分析不同节点之间的关系以获取全部区块的数据。在哈希算法中,若攻击者能够支配51%的区块,他就可以操纵整个区块链,从而能够随意篡改区块链中的数据。此外,在计算机科学中,匿名指的是无关联性的化名,也就是说,攻击者无法将用户与系统之间的任意两次交互进行关联[32]。但在区块链中,攻击者可以通过部署任意多的恶意节点监听网络通信信息,并将节点IP地址与链上交易、用户身份等进行关联[33]。因此,不同交易之间的关联极易被识别,危及区块链的匿名性。

区块链的共识机制存在再中心化的危险[34]。在区块链的运行中,节点的数量是一个问题——应该使用多少个节点来启动服务?应该接受多少数量的请求[35]?换言之,区块链能够容纳多少节点,满足多少请求?这与区块链的可扩展性息息相关。区块链运作规则的制定依靠节点间的共识,但经由共识所达成的规则只针对链上各节点,这难以保障链下公众的权益。例如,在传统市场实施一物多卖等类似"双花"的行为需要承担法律责任,而区块链仅阻止或纠正当次"双花"行为[36]。并且,技术精英在代码规则的制定和重大问题的决策中具有更大的话语权,其他参与者则没有机会对代码制定和系统运作提出意见和质疑。例如,2016年,构建在以太坊区块链上的应用程序"the DAO"源代码中的漏洞被利用,导致以太坊被盗价值5 000万美元的以太币。以太坊核心开发人员最终决定通过硬分叉返还被盗的以太币,强行将以太坊区块链分叉为两个不同的版本[15]。可见,基于分布式共识的网络并非平等的结构,在没有公共机构协调的情况下,大规模利用区块链技术容易导致新的寡头政治和社会的两极分化。

总体而言,区块链尚存在去中心化(Decentralization)、安全性(Security)、可扩展性(Scalability)不可兼得的问题。有学者借用金融领域的观点将这一问题称为区块链的"不可能三角"或"三元悖论",意指三个目标最多只能实现其中两个[37]。也就是说,区块链只解决了技术层面的问题,为促进政府数据开放提供了一种方案,但还面临着监管不足等法律层面的问题。因此,在对政府数据开放进行优化的过程中,既要克服技术无用论的盲目自大,又要破除技术决定论的乌托邦式臆断。

四、主权区块链:国家法律监管之下的技术治理

(一)主权区块链与政府数据开放的契合点

如上所述,在将区块链运用于政府数据开放的过程中,中心化的监管与去中心化的技术呈现出了各自的优势和劣势。因此,二者需要相互配合、补充,政府数据开放的制度设计应从"监管"思维转向"治理"思维。在此过程中,区块链可以被当作技术工具引入数据治理中,跳出现行政府数据开放的单一监管模式;但技术不能代替监管,面对技术无法解决的问题,政府应加强引导,而非缺位、让位。

在理论层面,贵阳市人民政府于 2016 年 12 月发布的《贵阳区块链发展和应用》白皮书中提出了主权区块链概念[38]。连玉明曾在"三部曲"中对主权区块链的相关知识进行了详细介绍[39-41]。在实践层面,得益于移动支付经验的积累和通信基础设施的完善,我国已经发行了国家法定数字货币(Digital Currency Electronic Payment,简称 DCEP)。与完全依托于去中心化区块链技术的私人数字货币不同,DCEP 属于主权区块链的应用,其通过中央银行担保并由国家信用支撑来保障定价和公信力,兼具"去中心化"与"中心化"的优势,从而能够填补主权国家在数字货币领域的监管空白。从初步试点、应用推广再到体系形成,我国正在积极开展主权区块链实践。"主权区块链将成为未来主权国家推动区块链发展的主流形态"[42]。因此,下文将引入主权区块链概念,尝试提出一种基于主权区块链的政府数据开放模式。具体而言,主权区块链与政府数据开放存在如下三方面契合之处。

首先,主权区块链的技术支撑是区块链,将主权区块链运用于政府数据开放属于技术层面的变革。与其他区块链一样,主权区块链的通讯、存储、安全、共识等机制能够为数据实时更新到链上提供渠道,并为所有节点共同参与数据维护扫清技术障碍,形成高效、透明的数据传输系统。在技术驱动下,区块链上各节点之间相互制约,减少了全能政府滥用权力的机会。单中心政府数据开放模式中一元主体支配、公众服从的封闭结构将被打破,数据开放不再聚焦于政府一端,而是通过促进各主体的主动参与以解决数据在不同政府层级、部门以及不同领域之间的传递难题。

其次,区块链只是一种技术工具,其应用须在国家主权范畴之下。尽管主权区块链"与其他区块链同样具有分布式、不可篡改、互相可信任、通过智能合约转移价值等特点,但却向区块链中注入了国家主权意志,加强了对区块链的政府监视、技术干预"[43]。主权是一个国家对其领土界限内的人、事、物等进行管控的权力。作为国家及其法律基础的主权具有不可分割的特征,因为一个主权国家无法同时拥有两个或以上的最高权威[44]。区块链的运用则经常伴随着反政府的言论,因为区块链技术具有专业性,其运行离不开代码规则,而该规则的制定权掌控在技术开发者手中,国家以及其他用户无法参与其中。这既会导致问责困难,还会滋生网络违法犯罪。并且,区块链的运行依托于自动化处理,但人类社会是高度复杂的系统,各部分之间存在着不可预测的非线性连接。我们必须防范过分简化复杂性和不加区分地应用自动程序的危险。为了确保区块链的正常运行,某种程度的监督仍是必要的。在此意义上,区块链只能是赋能者,而非决策者。主权区块链强调在维护国家主权的前提下,进一步对区块链进行法律监管,以提高数据通道的可信度。

最后,主权区块链的本质是一种科技与制度叠加的,具有分布式整合功能的治理技术。面对政府数据开放去中心逻辑与单中心逻辑的此消彼长,不同利益攸关者之间会出现摩擦和冲突。治理

(Governance)意味着分布与整合的统一。因此,只有通过治理才能切实保障区块链和政府数据开放的可扩展性。区块链技术的去中心化并不意味着要消解国家职能,而是为了促进更好地治理。在此意义上,区块链技术只应用于治理层面。基于主权区块链的政府数据开放治理要求更多具有参与性的政治实践,其既需要遵循区块链的逻辑,通过"去中心化"技术留给科技公司足够的创新空间,给个人足够的参与空间;同时又要将区块链置于主权框架下以保障国家对数据开放的监管,建构一个政府引导、节点共治的治理共同体,推动形成一条兼具去中心化、安全性和可扩展性的秩序链条,在可监管的基础上,实现数据的可分布。

(二)三元悖论的克服:主权区块链的三层结构

考虑到去中心化、安全性和可扩展性之间的权衡难题,可以将主权区块链理解为一种多区块链结构。具体而言,区块链主要包括许可型区块链(私有的、受限的,需要由特定机构授权访问)和非许可型区块链(公共的,向所有人开放)[45]。其中,公有链(Public Blockchain)属于非许可型区块链,许可型区块链分为私有链(Private Blockchain)与联盟链(Consortium Blockchain)。

第一,将公有链运用于政府数据开放时,其由面向公众的若干节点构成,这可以保障区块链的去中心化。在公有链中,任意节点均有权写入、读取数据。因此,在政府数据开放中,可以通过公有链开辟数据惠民新路径。就数据写入而言,公有链是对外开放的,它的去中心化特性与海量、分散的数据相契合。基于此,用户无须事先注册、登录就可以将拟上传的数据封装于数据区块中,将意见反馈至链上,这有利于满足多元主体的数据诉求。同时,公有链可以通过工作量证明等方式激励节点作出贡献,以提升多元主体分享数据的积极性。就数据读取而言,存储在公有链上的数据将经由P2P网络广播至各个节点,政府部门对用户意见的回应等相关政务信息也可以通过公有链向社会公开,提高了数据和流程的透明度。

第二,将私有链运用于政府数据开放时,其由单个政府部门构成,保障了区块链的安全性。私有链是只对单个组织(例如,保密局)开放的封闭式区块链,其中数据的写入和读取受到高度限制。因此,私有链的价值在于提供一个可靠的专网环境,以防范内外部对数据的攻击,从而抵御数据风险。这也为应对公有链在数据传输中的"木桶效应"提供了解决方案。也就是说,公有链上数据的处理效率受制于最弱节点,但私有链拥有对节点的完全控制权。与公有链相比,难以受到外部因素影响的私有链更为高效、可控。与联盟链相比,私有链从基础架构而非组织机构出发来对数据进行调控,从技术层面进一步保障了数据安全。

第三,将联盟链运用于政府数据开放时,其由多个政府部门构成,保障了区块链的可扩展性。联盟链兼具私有链的集中特征与公有链的分布特征,体现出"有限去中心化"的色彩,其优势具体表现为如下两方面:一是健全数据交流机制,促进政府横向、纵向的数据共享。虽然政府各部门在履职中积累了大量数据,但囿于科层体制的局限,数据在政府内部纵向传递时容易失真、延迟,而在横向流通时则受制于制度壁垒、部门利益。因此,不同政府部门存储着大量异构数据,形成了一个个数据孤岛。联盟链可以为政府提供一个跨地区、跨层级、跨部门的分布式数据共享平台,打破部门间"各自为政"的数据乱象。二是营造数据规制空间,保障区块链上、链下的规则协同。面对区块链中政府权力的私主体化和技术精英的再中心化危险,需通过联盟链加强法律规制。联盟链是分布的,但其仅限于少数受信任的节点访问。基于此,政府部门可以在必要时通过人为干预来为数据开放营造规制空间,将链下法律"映射"至链上。在链上规则无法保障链下公众权益的地方,实现技术

规则与法律制度的相辅相成。

可见,根据开放程度的不同,区块链被细分为公有链、私有链以及联盟链三种具体类型。基于主权区块链的政府数据开放可以根据不同的数据类型、应用场景选择合适的区块链类型,以充分发挥各类区块链的优势,构建一个由面向政府各部门的联盟链、面向单个政府部门的私有链,以及面向大众的公有链所组成的主权区块链。

(三)基于主权区块链的政府数据开放构造

综合上文,主权区块链应是一个"以链治链"的多区块链系统,该系统由公有链、联盟链、私有链三个维度(层次)共同塑造而成,其具体构造如图 3 所示。通过多层协作,与政府数据开放相关的各个利益主体均可被置于互联、并行的主权区块链中,形成由政府引导、多元主体参与的政府数据开放治理格局。

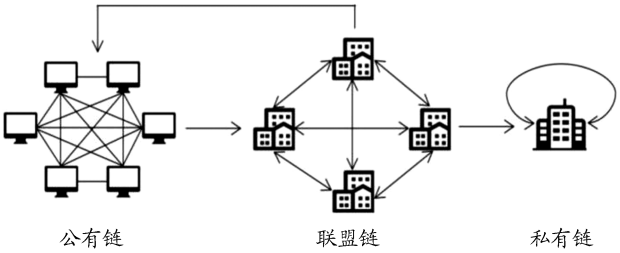

图 3　基于主权区块链的政府数据开放治理模式

1. 搭建社会公众的公有链平台

在主权区块链中,各主体具有唯一的身份标识码(Identity Document,简称 ID)。根据 ID 的不同,各主体将被划分到不同类型的区块链中。相应地,社会公众(个人或企业)会被划分到主权区块链的基础层——公有链上。公有链的核心特征是分布和开放。依托于 P2P 网络和共识算法,公有链能够在广泛、分散的多元节点之间创建数字分类账,该账本不为中心服务器所控制,而是由每个地位对等的节点共享,并为其提供写入和读取数据的渠道,从而降低公众参与数据开放的门槛。基于激励机制,可以给予用户一定权益以鼓励其参与数据开放,从中吸纳更优质的数据资源,激活用户数据市场。

公有链塑造了一个有助于底层数据融通共享的平台,但缺陷在于,它的去中心化特征会带来数据处理的低效和监管问题。公有链在实现更高参与度的同时造成了更长的延迟。此外,正如阿特佐伊所言,在去中心化的自治组织中,个人始终生活在一种不稳定的前主权状态[12]。政治被简化为经济人的游戏,旨在最大化参与者(尤其是少数有影响力的参与者)的效用。在公有链中,个人不是公民,而只是消费者。他们进入和退出区块链的成本相对较低。这会导致"权力的自由浮动",催生出许多基于"共识"的冲突团体。换言之,仅通过公有链达成共识是不够的,它并不能解决争端、实施监管。基于主权区块链的解决方案需要引入一个协调点。由于公有链是直接向公众开放的,这也有利于其他类型区块链的接入,以进一步实现链和链之间的对接。

2. 推进协同机构的联盟链治理

根据 ID 识别,相关政府部门会被划分到主权区块链的中间层——联盟链上。联盟链将参与节点限定在有限范围内以提高数据处理效率,据此构建政府部门之间的数据协同共享平台。例如,有学者认为,可以在部门间构建以业务为划分的交通链、税务链、医疗链等联盟链[46]。基于联盟链,不

同地区、层级的相关部门将建立联结,各个具有记账权的部门可以实时将政务数据共享至链上,其他部门则能够全流程、可追溯地掌握一手数据,并基于算力奖励而主动对数据进行核查、去伪。各部门无须依托于中心服务器,在本地即可实现数据的跨部门传输,从而简化数据交互的流程。此外,在联盟链中,还须在基于参与节点共识的智能合约中预先写入数据的类型、格式、权限、更新频率等统一规则以健全数据共享标准,打破部门间的数据壁垒。基于智能合约,系统将自动评估数据;若数据不符合既定标准,系统便会根据协议向各参与节点发布警示,以实现部门间的联合惩戒。

除了通过完善技术措施以实现机构协同外,还需利用联盟链建立起灵活的政府数据开放治理框架。公有链和联盟链中蕴含的去中心特性只是技术层面的去中心化。公有链的绝对开放容易引发技术风险。劳伦斯·莱斯格将试图打造"没有法律的世界"的自治说归结为"早期互联网的梦想",他认为这种"网络空间无法被规制"的观点是错误的,实际上法律在物理世界和数字世界都能得到适用[30]320-323。在联盟链接入公有链之前,公有链仍缺乏相应的法律保障。因此,在政府数据开放中,还要通过联盟链构建起"法链",重新引入国家控制的要素,以解决公有链过度去中心化所带来的监管不足的问题。凯文·沃巴赫通过列举R3金融行业协会项目(Corda)来说明法律与分布式分类账的协作关系。使用分布式分类账技术的Corda网络明确允许监管者介入,并使其操作"监督观测节点",以获取实时交易信息,从而促进有效监管[47]。可见,监管机构可以作为联盟链的参与者加入系统的运行和维护[48]。

虽然联盟链受个别预选节点控制,但其始终无法脱离去中心化的技术架构。例如,由国家信息中心领导的联盟链——区块链服务网络(BSN)的基础设施层既支持专有网络、公有云、私有云等部署形态,也支持跨网混合部署[49]。因此,在基于主权区块链的政府数据开放中,联盟链面对的是整个区块链网络,而非局限于单一或部分节点。其中包含两层含义:一方面,联盟链要基于区块链的基础结构发挥"内嵌式"监管作用,通过动态监管扫清因技术局限而无法覆盖的监管盲点。另一方面,联盟链中还蕴含着数据监管思维向治理思维的转变。在将联盟链与公有链进行对接之后,可以为公众提供政府数据查询和意见反馈的平台,以提高数据的透明度和公众的参与度。各主体不再受限于中心权威,而是能够在可信数据的基础上实现直接的交互和连通。在此意义上,政府只是参与者和协调者,而非领导者,其侧重于发挥引导和推动作用,而非强制作用。

3. 筑牢职能部门的私有链隔离

根据ID识别,单个职能部门会被划分到主权区块链的隔离层——私有链上。私有链具备只对特定主体开放的、封闭的环式结构,其中数据无法向外流通。私有链通过如下两个步骤打造数据的隔离装置。一是分流敏感数据。政府数据种类繁多,因此须预先明确数据开放的范围,建立数据分类分级制度。私有链可用于分流不予开放的政府数据。政府部门在对外开放数据前,可直接借助私有链分流涉及个人隐私、危及国家安全的敏感数据。另外,联盟链是公有链和私有链之间的桥梁,公有链上的数据将受到联盟链的检验。根据联盟链确定的数据分类标准,非敏感数据或经过脱敏处理后符合开放条件的数据将由P2P网络广播至各个节点,而敏感数据则保留在私有链上。二是保障数据安全。首先,须通过密码学技术、块链式数据结构对被分流的敏感数据进行加密存储。采用哈希算法将敏感数据转化为难于识别、易于存储的哈希值,以达到数据脱敏的效果。利用非对称加密技术使数据只对具有访问资格的人员开放,赋予其公私钥双重保护。在数据被加密后,再对其进行块链式存储,以提供稳定的数据存储环境。其次,须通过智能合约、时间戳等技术对已存储

的敏感数据进行实时监测。私有链内的数据流转依托于安全传输协议,以验证系统中的数据访问请求和操作是否符合标准。一旦出现非法行为,带有相应用户 ID 的操作记录将会被自动上报,并触发拒绝访问的装置。任何试图篡改、损坏、删除、窃取数据的行为都将被相关部门及时发现、处置。而时间戳技术则可以保证数据留痕,实现数据流转全过程的可追溯和可问责。

综上所述,政府数据开放是顺应时代发展的重大举措,其目的在于促进数据流通,转变政府职能。现行政府数据开放所采用的"集中-分布"模式依托于现实的单中心权威,但无边无垠的数据流已经打破了物理空间与虚拟空间的界限。区块链无疑为破解政府数据开放的单中心困境提供了技术上的解决方案,为对虚拟的数据流通进行规制提供了突破口。但单独依凭区块链的政府数据开放容易陷入技术决定论的泥沼,无法克服去中心化、安全性与可扩展性的三元悖论。在此背景下,主权区块链的提出切合时宜。在基于主权区块链的政府数据开放中,以链治链的策略既为数据自由流通提供了广阔的平台,也为主权国家对多元空间的治理提供了思路。

参考文献:

[1]李海敏. 我国政府数据的法律属性与开放之道[J]. 行政法学研究,2020(6):144-160.

[2]ALZAMIL Z S,VASARHELYI M A. A new model for effective and efficient open government data[J]. International Journal of Disclosure and Governance,2019,16(4):174-187.

[3]陈尚龙. 论政府数据开放的理论基础[J]. 理论与改革,2016(6):104-107.

[4]沈亚平,许博雅."大数据"时代政府数据开放制度建设路径研究[J]. 四川大学学报(哲学社会科学版),2014(5):111-118.

[5]岳丽欣,刘文云. 我国政府数据开放平台建设现状及平台框架构建研究[J]. 图书馆,2017(2):81-85,107.

[6]杨瑞仙,毛春蕾,左泽. 我国政府数据开放平台建设现状与发展对策研究[J]. 情报理论与实践,2016(6):27-31.

[7]郑磊,高丰. 中国开放政府数据平台研究:框架、现状与建议[J]. 电子政务,2015(7):8-16.

[8]吴旻. 开放数据在英、美政府中的应用及启示[J]. 图书与情报,2012(1):127-130.

[9]ABDUGAFFAROVICH A A,ABBASOVICH V A,BAKHTIYAROVICH N N. E-government,open data,and security:Overcoming information security issues with open data[J]. Computer Science and Information Technology,2015,3(4):133-137.

[10]余奕昊,李卫东. 我国地方政府数据开放平台现状、问题及优化策略:基于 10 个地方政府数据开放平台的研究[J]. 电子政务,2018(10):99-114.

[11]潘祥辉. 去科层化:互联网在中国政治传播中的功能再考察[J]. 浙江社会科学,2011(1):36-43,156.

[12]ATZORI M. Blockchain technology and decentralized governance:Is the state still necessary? [J]. Journal of Governance and Regulation,2017,6(1):45-62.

[13]FAN L J,GIL-GARCIA J R,SONG Y,et al. Sharing big data using blockchain technologies in local governments:Some technical,organizational and policy considerations[J]. Information Polity,2019,24(4):419-435.

[14]黄如花,王春迎. 我国政府数据开放平台现状调查与分析[J]. 情报理论与实践,2016(7):50-55.

[15]Van PELT R,JANSEN S,BAARS D,et al. Defining blockchain governance:A framework for analysis and comparison[J]. Information Systems Management,2021,38(1):21-41..

[16]何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017(4):1-7,15.

[17]韩璇,袁勇,王飞跃. 区块链安全问题:研究现状与展望[J]. 自动化学报,2019(1):206-225.

[18]程啸. 区块链技术视野下的数据权属问题[J]. 现代法学,2020(2):121-132.

[19]石超. 区块链技术的信任制造及其应用的治理逻辑[J]. 东方法学,2020(1):108-122.

[20]大数据战略重点实验室. 块数据 3.0:秩序互联网与主权区块链[M]. 北京:中信出版社,2017.

[21]武岳,李军祥. 区块链 P2P 网络协议演进过程[J]. 计算机应用研究,2019(10):2881-2886,2929.

[22]蔡晓晴,邓尧,张亮,等. 区块链原理及其核心技术[J]. 计算机学报,2021(1):84-131.

[23]袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报,2018(11):2011-2022.

[24]徐琳,袁光. 区块链:大数据时代破解政府治理数字难题之有效工具[J]. 上海大学学报(社会科学版),2020(2):67-78.
[25]邵奇峰,金澈清,张召,等. 区块链技术:架构及进展[J]. 计算机学报,2018(5):969-988.
[26]魏松杰,吕伟龙,李莎莎. 区块链公链应用的典型安全问题综述[J]. 软件学报,2022(1):324-355.
[27]郑戈. 区块链与未来法治[J]. 东方法学,2018(3):75-86.
[28]KIVIAT T I. Beyond bitcoin:Issues in regulating blockchain transactions[J]. Duke Law Journal,2015,65(3):569-608.
[29]KSHETRI N. Blockchain's roles in strengthening cybersecurity and protecting privacy[J]. Telecommunications Policy,2017,41(10):1027-1038.
[30]劳伦斯·莱斯格. 代码 2.0:网络空间中的法律[M]. 修订版. 李旭,沈伟伟,译. 北京:清华大学出版社,2018.
[31]孙琳,邓天奇. 区块链赋能数字出版:逻辑耦合、技术应用及风险审视[J]. 数字图书馆论坛,2022(12):54-60.
[32]张宪,蒋钰钊,闫莺. 区块链隐私技术综述[J]. 信息安全研究,2017(11):981-989.
[33]曹雪莲,张建辉,刘波. 区块链安全、隐私与性能问题研究综述[J]. 计算机集成制造系统,2021(7):2078-2094.
[34]黄运康. 从代码到法律:区块链平台数字竞争规则的建构[J/OL]. 重庆大学学报(社会科学版):1-14. [2023-10-09]. http://kns. cnki. net/kcms/detail/50. 1023. C. 20220309. 1022. 002. html. Doi:10. 11835/j. issn. 1008-831. fx. 2022. 03. 002.
[35]CLAVIN J,DUAN S S, ZHANG H B, et al. Blockchains for government:Use cases and challenges[J]. Digital Government: Research and Practice,2020,1(3):1-21.
[36]许荻迪. 自治与他律:平台二重性视角下的区块链治理[J]. 改革,2020(8):68-82.
[37]刘炼箴,杨东. 区块链嵌入政府管理方式变革研究[J]. 行政管理改革,2020(4):37-46.
[38]贵阳市人民政府新闻办公室. 贵阳区块链发展和应用[EB/OL]. (2017-02-17)[2023-10-09]. https://www. sohu. com/a/126543390_353595.
[39]连玉明. 主权区块链 1.0:秩序互联网与人类命运共同体[M]. 杭州:浙江大学出版社,2020.
[40]连玉明. 主权区块链 2.0:改变未来世界的新力量[M]. 杭州:浙江大学出版社,2022.
[41]连玉明. 主权区块链 3.0:共享秩序下的全球治理重构[M]. 杭州:浙江大学出版社,2023.
[42]高奇琦. 主权区块链与全球区块链研究[J]. 世界经济与政治,2020(10):50-71,157-158.
[43]季卫东. 主权的嬗变:数字化"魔兽世界"与法律秩序创新[J]. 交大法学,2023(5):5-17.
[44]匡梅. 跨境数据法律规制的主权壁垒与对策[J]. 华中科技大学学报(社会科学版),2021(2):96-105.
[45]TSHERING G,GAO S. Understanding security in the government's use of blockchain technology with value focused thinking approach[J]. Journal of Enterprise Information Management,2020,33(3):519-540.
[46]杨杨,杨加裕. 构建基于主权区块链的税收信用体系研究[J]. 税收经济研究,2019(6):60-68.
[47]凯文·沃巴赫. 链之以法:区块链值得信任吗?[M]. 林少伟,译. 上海:上海人民出版社,2019:81-82.
[48]洪学海,汪洋,廖方宇. 区块链安全监管技术研究综述[J]. 中国科学基金,2020(1):18-24.
[49]袁煜明,王蕊,孟岩,等. 区块链产业应用 100 例[M]. 北京:人民邮电出版社,2021:85.

Sovereign blockchain: An innovative governance model of government data opening

KUANG Mei

(*KoGuan School of Law, Shanghai Jiao Tong University, Shanghai 200030, P. R. China*)

Abstract: The current concentration-distribution model of government data opening not only has the chronic disease of over centralization, but also is difficult to ensure the overall effect of data distribution. In the process of data concentration, the data of multiple nodes is difficult to converge to the central node. In the process of data distribution, the data of central node is difficult to transfer to multiple nodes; In the process of data utilization, multiple nodes are difficult to interact with the central node. In view of this, it is necessary to change the current model of government data opening and seek a new technical support for it. Blockchain is an

ideal technology to solve the problem of government data opening. Through four kinds of mechanisms including communication, storage, security, consensus, blockchain can ensure data flow, overcome single point of failure and bureaucratic organization limitations as well as promote the government to change its functions and enable multiple subjects to participate in data opening. However, when the single blockchain technology is applied to the opening of government data, it is still in danger of circumventing supervision, solidifying errors, cracking algorithms and re-centralization. There are problems that decentralization, security and scalability cannot be realized at the same time. Facing the technical demand of government data opening and the ternary paradox of blockchain technology, this paper introduces the concept of sovereign blockchain to explore the path of government data opening that can realize the compatibility of centralized sovereign state supervision and decentralized blockchain technology. There is a connection between sovereign blockchain and government data opening. Sovereign blockchain is a governance technology which can integrate institution and technology as well as has the function of distributing and concentrating. Relying on sovereign blockchain, we can build a government data opening model with government guidance and joint governance of nodes. Specifically, sovereign blockchain is composed of public blockchain, consortium blockchain and private blockchain. This structure helps to overcome the ternary paradox of single blockchain technology. Therefore, in the process of government data opening, we can choose appropriate blockchains according to different data types and application scenarios, and then create a sovereign blockchain of chain governance by building a public blockchain platform for the public, promoting the consortium blockchain governance of collaborative institutions, and strengthening the private blockchain isolation of functional departments. In government data opening based on sovereign blockchain, the public blockchain with distributed and open characteristics is conducive to the sharing of underlying data and the access of the consortium blockchain. The consortium blockchain can not only build a data sharing platform between government departments by limiting the participating nodes to a limited range, but also establish a legal chain by embedding the public blockchain, and place the blockchain under the sovereignty framework to ensure national supervision. The data on the public blockchain will be tested by the consortium blockchain, in which sensitive data will be retained on the private blockchain, and other data will be transmitted to the public from the public blockchain. The private blockchain is used to provide a secure storage environment for the diverted sensitive data.

Key words: government data opening; blockchain; sovereign blockchain; legal governance; chain governance

(责任编辑　胡志平)