区块链技术视野下的数据权属问题

程 啸

【摘 要】区块链中的数据权属问题仅指用户上链的特别数据即事务数据、实体数据和合约数据的归属。应区分公有链、联盟链和私有链，分别研究各自的数据权属。公有链中，因不存在中心式数据控制者，也无收集处理数据的行为，任何节点或用户对于共有链上记载的非自己上传的数据均不享有民事权益。联盟链和私有链中，参与成员可对数据的权属与利用进行约定。区块链上的政务数据归国家所有。

【关 键 词】区块链；数据；权属；收集；处理

【作者简介】程啸(1976-)，男，江西九江人，教育部长江学者青年学者，清华大学法学院教授，法学博士(北京 100084)。

【原文出处】《现代法学》(重庆)，2020.2.121～132

【基金项目】2018年度国家社科基金重大项目“大数据时代个人数据保护与数据权利体系研究”(18ZDA146)；清华大学自主科研计划文科专项“中国民法典侵权责任编立法研究”(2017THZWYY14)。

引言

区块链被认为是互联网问世后信息技术领域最重要的技术。区块链是一个去中心化的分布式数据库，该数据库由一串使用密码学方法产生的数据区块有序连接而成，区块中包含一定时间内产生的无法被篡改的数据记录信息。[①]由于区块链技术是一种去中心化的数据记录与存储体系，该系统本身有很强的可信赖性，有效地解决了人们之间的信任问题，故此，尽管区块链产生的初衷是为比特币等数字货币提供技术支撑，但该技术的应用范围和场景远大于此。目前区块链技术的应用已延伸到数字金融、物联网、智能制造、供应链管理、数字资产交易等多个领域，包括我国在内的许多国家也都高度重视区块链技术的发展与应用。

因区块链技术建立的系统具有高度的可信赖性，故在可预见的未来，区块链技术将在社会生活的各个领域被广泛运用，如将区块链技术运用于教育、就业、养老、精准脱贫、医疗健康、商品防伪、食品安全、公益、社会救助等领域，可以为大众提供更智能、便捷、优质的公共服务。再如，通过区块链数据共享模式，可以有效地实现政务数据跨部门、区域的共同维护和利用，促进业务协同办理，更好地为公众提供政务服务。

区块链技术本身不是万灵丹。区块链技术的广泛运用及其与人工智能、大数据、物联网等前沿信息技术的深度融合，也产生了不少新的法律问题。例如，区块链技术与隐私权、个人信息保护就存在矛盾。区块链上的信息几乎无法被修改，一旦有人将他人隐私或个人信息以一条交易信息的附加信息记载于以太坊的公链上，就没有人可以将这条信息加以删除，该信息将永远存在于以太坊的公链上。[②]欧盟通过的《通用数据保护条例》确立的擦除权、被遗

忘权在区块链内更是无法实现,因为系统旨在防止它这样做。[③]再如,与传统自动化或非自动化收集数据信息不同的是,区块链是去中心化的,并不存在中心式数据控制者,因此区块链上的数据究竟归谁,何人对之享有何种民事权益,也是急需研究的法律问题。要使区块链这项变革性技术能够被科学合理的加以运用,就应当研究解决其产生的各种法律问题。"法律是区块链的必由之路,而非其毁灭的根源……就网络层面而言,区块链的确可以称得上是商业、政府和社会的变革性技术,但前提是要与法律和谐共存。"[④]有鉴于此,本文将对区块链技术运用中各界普遍关注的一个问题即区块链上的数据权属问题进行初步的研究。文章的第一部分对大数据时代背景下中心式数据控制者对其合法收集的数据所享有的权益进行简单介绍。因为,无论区块链上还是区块链下,数据的归属都有激烈的争论,这是共性问题。第二部分将在区分不同的区块链类型及其上数据种类的基础上,依次讨论公共区块链、联盟链及私有链上的数据归属。第三部分对区块链中政务数据的权属进行分析。最后是文章的结论。

一、中心式数据控制者的数据权属

大数据时代中的数据蕴涵着巨大经济价值和战略价值,不仅成为企业、政府的重要资产,也是国家的重要战略资源。[⑤]然而,对于大量收集处理数据的企业和政府,其对合法收集和处理的数据究竟享有何种权益,却缺乏明确的法律规定。我国目前唯一对数据做出规定的法律是《民法总则》,该法第127条规定:"法律对数据、网络虚拟财产的保护有规定的,依照其规定"。这一原则性规定的立法理由在于:"鉴于数据和网络虚拟财产的复杂性,而限于《民法总则》的篇章结构,如何界定数据和网络虚拟财产的,如何规定数据和网络虚拟财产的权利属性和权利内容,应由专门法律加以规定",《民法总则》该规定,"一方面确立了依法保护数据和网络虚拟财产的原则,另一方面,鉴于网络和虚拟财产权利性质存在争议,需要对数据和网络虚拟财产的权利属性作进一步深入研究,进一步总结理论和司法实践的经验,为今后立法提供坚实基础。"[⑥]立法上对于数据权属的不明确,也给理论界探讨数据权属问题提供了空间。

目前,对数据权属的研究主要集中在数据企业对其合法收集和处理的数据享有何种民事权益的问题之上。实务界主流观点认为,现行法体系下应通过《反不正当竞争法》对数据控制者的权益加以保护。数据控制者累积的大量数据是其通过长期的合法经营并投入大量的人力、物力和财力积累所致,这些数据是企业在市场竞争中的竞争优势。《反不正当竞争法》要保护诚实经营和公平竞争的市场经济秩序,禁止那些不劳而获搭便车给他人权益造成损害的行为。[⑦]故此,应当通过该法第2条第2款承认并保护数据控制者对数据的合法权益。目前,已经发生的一些数据权属纠纷案件中,法院基本上采取的是该观点。[⑧]从比较法来看,美国和欧盟的学者中也有类似的观点。[⑨]

在理论界,不少学者认为,以《反不正当竞争法》来保护数据控制者实际上等于将数据控制者的数据权利降格为一种受法律保护的纯粹经济利益,只能在其遭受特定方式侵害的时候获得救济,保护的强度和密度显然不足。此种保护方法既不利于数据的流动和分享,也无法充分地鼓励数据控制者更多地收集处理数据。[⑩]故此,应当承认数据控制者对其合法收集、存储的数据享有某种新型的财产权利,并赋予其排他效力和绝对权保护请求权。[⑪]

笔者赞同将数据控制者的数据权利界定为一种新型的财产权利。首先,数据控制者之所以可以取得数据权利,是因为其通过合法的且支付对价的收集与处理,原始取得了以其所收集和处理的数据为客体的新型财产权利。数据控制者对合法收集的个人数据享有应受到法律保护的权利。该权利既不依赖于被收集者的授权,也不依赖于其他在先权利或许可,而是原始取得的权利。一方面,就个人数据而言,数据控制者依据法律规定,在公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被

收集者同意收集个人数据的行为是合法的事实行为;另一方面,数据控制者收集处理个人数据时要付出相应的成本,向被收集者支付了相应的对价,符合公平原则,应当产生相应的民事权利。

其次,法律是否将特定利益作为一种财产权加以保护,取决于法律想用财产权这一工具达成何种法政策目标。“在人们眼中,财产权是什么,取决于人们想用财产权做什么——换言之,人们所欲达成之目的决定了财产权的类型、形式与内容。”[12]数据控制者对其收集、存储和加工的数据资产是否享有新型财产权利,主要取决于法政策目标是鼓励还是限制数据产业的发展。至于数据权利在多大程度上符合传统民法权利客体的要求,则属于立法与司法技术的范畴。尽管通过反不正当竞争法可以在一定程度上给予数据控制者一定的保护,但是此种保护是消极的、被动的,是在受到侵害时的救济,并未对数据控制者进行赋权。数据控制者对于数据有各种合法的可能使用方式。在没有界定数据权属的前提下,很难形成一个稳定有效的激励机制,使数据企业更好的利用数据,也无法建立一个用于配置数据资源的有效市场。

最后,从《民法总则》第127条的体系位置来看,立法者在紧接着人格权、物权、债权和知识产权之后规定对数据的保护,实际上等于认同了数据上的权益是一种新型的财产权益。当然,具体应当如何确定此种数据权益的性质、内容以及保护方法等,还需要进一步研究并通过相应法律加以明确。

二、不同类型区块链上的数据权属

(一)去中心化的区块链中数据权属问题的特殊性

当前人们对数据权属的讨论都是以数据收集和处理者处于中心地位为场景的。也就是说,无论是自动化还是非自动化的数据收集处理,数据都只是单向度的从信息主体流向数据的收集处理者的,始终有一个中心式的数据控制者。它们可能是各类网络公司等数据企业,也可能是各种国家机关。这些数据收集处理者在为他人提供网络或政务服务的同时,不断地收集处理服务对象的数据。是否收集、如何收集、怎样处理等问题的决定权都是在数据收集处理者的手中。在这种“数据被收集者—数据收集者”的双边关系中讨论数据权属问题,虽有争议,但并不困难。因为,即便认定数据企业或政府机关对于数据享有相应的民事权益,也可以通过赋予数据被收集者相应的权益(如个人信息权)来平衡二者的关系。例如,欧盟《通用数据保护条例》就赋予了用户访问权、更正权、删除权以及反对权等直接指向数据控制者的权利,从而实现用户对数据的控制,保护其权利。[13]这种权利义务构造针对的是中心式数据控制者的场景。

然而,去中心化的区块链中并不存在中心式的数据控制者。区块链作为公共数据库记录了网际间所有的交易信息,并随时更新,每个用户都可以通过合法的手段从中读取信息、写入信息。因此,讨论区块链中数据的权属问题时无法基于双边的关系。这就产生了两个问题。其一,在区块链上写入信息(或输入数据)的用户,对于区块链上的数据是否享有权益以及享有何种权益?其二,既有的用于解释中心式数据控制者对数据享有权益的各种理论,能否同样适用于区块链技术视野下对数据权属问题的解释或作为正当化的基础呢?

(二)区块链及其上数据的类型

区块链上的数据很多,[14]但总体上可以分为账户数据、区块数据、事务数据、实体数据、合约数据、配置数据等。[15]其中,(1)账户数据是描述区块链事务的实际发起者和相关方的数据,区块中记录的事务信息均被关联到相关的账户之上,每个区块链服务客户拥有一个或多个账户来使用区块链服务;(2)区块数据是区块链网络的底层链式数据,用来把一段给定时间内发生的事务处理结果持久化为成块链式数据结构;(3)配置数据是区块链系统正常运行过程中所需的配置信息;(4)事务数据是描述区块链系统上承载的具体业务动作的数据,既包括交易类型事务,也包括非交易类型事务;(5)实体数据是描述事务的静态属性的数据,通常包括发起方地址、接收方地

址、交易发生额、交易费用、存储数据和实体数据备注;(6)合约数据是描述事务的动态处理逻辑的数据。

由于区块数据与配置数据属于基础性与结构性的数据,是某一区块链的共通数据。因此,这些数据只对区块链的底层程序结构具有意义,本身没有其他商业价值。事务数据、实体数据与合约数据与该区块链的应用和功能密切相关,即区块链用户利用区块链技术所上传的数据。因此,所谓区块链中的数据权属实际只是指用户上链的特别数据即事务数据、实体数据和合约数据的归属问题。

目前,已知的区块链技术大体可以分为三类。一是公共区块链(Public Blockchain),也称"公有链",即任何人都可以参与区块链数据的维护和读取,不受任何单个中央机构的控制,数据完全开放透明的区块链。此类区块链最典型的应用就是比特币系统、以太坊。[16]二是共同体区块链(Consortium Blockchain),也称联盟链,是指参与区块链的节点是事先选择好的,节点间通常有良好的网络连接等合作关系。至于区块链上的数据可以是公开的,也可以是内部的。此类区块链与公共区块链不同的是,其仅仅是部分去中心化。[17]例如,联盟链的运用场景如多家银行之间的支付结算或者多个企业之间物流供应链,政府之间的信息互通共享等。三是私有区块链(Private Blockchain),也称私有链,属于联盟链的一种特殊形态。私有区块链仅仅在组织内部使用,参与的节点只有有限的范围,如政府部门的内部管理、企业内部的票据管理等。因此,在私有区块链中,对于数据的访问和使用都有严格的限制。在完全私有的区块链中,写入的权限只限于参与者,而读取的权限可以对外开放,也可以随意加以限制。与公有链和联盟链相比,私有区块链的数据不存在无法篡改的特性,但具有更高效和更安全的隐私保护等优点。[18]

(三)公共区块链上的数据权属

在公共区块链中,用户将事务数据、实体数据或合约数据"上传"至区块链的技术,本质上是通过特定的哈希算法和默克尔树数据结构,将一段时间内接收到的交易数据和代码以及其他任意数据封装到一个带有时间戳的数据区块中,并链接到当前最长的主区块链上,形成最新的区块。[19]基于公共区块链所具有的"完全去中心化"分布式数据库的技术特征,笔者认为,任何节点或区块链用户对于公共区块链中的数据,均不享有如同中心式数据控制者对其合法收集、支付对价的数据集合那样相同或相似的财产权利。理由阐述如下:

首先,与中心式数据控制者单向收集处理用户的数据所不同的是,在公共区块链中,完全不存在中心式的数据控制者进行数据的收集和处理。由于区块链系统的节点一般具有分布式、自治性、开放可自由进出等特性,因而,一般采用对等式网络(Peer-to-Peer network,P2P网络)来组织分散的参与数据验证和记账的节点。P2P网络中的每个节点均地位对等且以扁平式拓扑结构相互连通和交互,不存在任何中心化的特殊节点和层级结构,每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点等功能。因此,在整个过程中,均不会涉及中心化的第三方,也不会在一个中心化服务器中存储任何数据。[20]

公共区块链的用户将数据上传至区块链包括以下两个环节:第一,任一区块数据生成之后,将由生成该数据的节点广播到全网其他所有的节点来加以验证。第二,P2P网络中的每个节点都时刻监听区块链网络中广播的数据和新区块,节点接收到邻近节点发来的数据后将首先验证该数据的有效性。如果数据有效,则按照接受顺序为新数据建立存储池以暂存尚未记人区块的有效数据,同时继续相邻近节点转发;如果数据无效,则立即废弃该数据,从而保证无效数据不会在区块链网络继续传播。[21]

因此,从公共区块链的数据层与网络层设计机理可见,其属于典型的分布式大数据技术。由于全网数据同时存储于去中心化系统的所有节点上,所以即使部分节点失效,只要仍存在一个正常运行的节点,区块链主链数据就可完全恢复而不会影响后续区块数据的记录和更新。这种高度分散化的区块链存储模式与传统意义上的大数据存储模式的不同

之处在于:后者是基于中心化结构基础上的数据备份模式,前者则是完全"去中心化"的存储模式。换言之,基于区块链技术的数据上传与共享技术并未将数据存储在任何一个中心机构的服务器上,而是所有的区块链用户均同时存储了区块链上的所有数据。

其次,在公共区块链中,也不存在数据的收集过程。中心式数据控制者之所以主张要对其合法收集处理的数据赋予相应的民事权益,根本原因就在于其从事了收集处理数据的过程,为此付出了劳动,支付了成本,而这些被收集和处理的数据也因此成为网络公司等数据控制者的重要资产。大体来说,中心式的数据控制者收集数据的技术过程包括:(1)数据控制者通过各种传感器、射频识别(RFID)、数据检索分类工具及移动设备的应用软件等采集使用网络服务的用户和其他民事主体的数据;(2)采集到数据后,数据控制者会把各种各样、结构复杂的数据转换为单一的或便于处理的结构,且在数据处理的过程中设计一些数据过滤器,通过聚类或关联分析的规则方法进行数据清洗(Data Cleaning),对数据进行重新审查和校验,删除重复信息、纠正存在的错误并提供数据一致性;(3)被整理好的数据将进行集成和存储。其中,数据处理与集成是非常重要的一步,如果单纯随意地放置数据,很容易产生数据访问性的困难,导致采集的数据无法利用。[22]由此可见,所谓"数据收集",并非简单随意地采集和存储数据,而是在采集之后,通过一定的技术手段对数据进行初步加工,从而形成有利用可能性的数据集合。

但是,在区块链技术下,某一节点对于其接收的数据进行验证并且暂存在区块链的行为,[23]并不具有数据控制者进行数据收集的技术特征。一方面,各个节点对数据进行接收和验证的行为,只是采取一定的技术手段对生成的区块数据的合法性进行验证,例如,采取工作量证明,即各个节点消耗自身算力尝试不同的随机数,进行指定哈希计算并不断重复该过程直至找到合理的随机数,随后生成区块信息,记录交易数据。[24]该过程并不对数据进行初步处理和清洗,只是将原始交易数据记入区块链而已。另一方面,最终记入区块链的交易数据也并非存储在某一个节点的服务器上,而是同步地在各个节点上均出现的相同数据。显然也不同于数据控制者收集数据后将之存储在自己的服务器或者进行云存储。

因此,如果说数据控制者对于其所合法收集的数据享有新型财产权利,是因为数据控制者在收集数据的过程中付出劳动,[25]那么,公共区块链上的各个节点对区块数据的接收和验证本身既没有对数据本身产生任何收集加工活动,也没有任何一个节点能够对数据进行排他的控制。所以,区块链的网络用户对于区块数据不可能享有如同中心式数据控制者那样的数据权利。

最后,是否向数据被收集者支付对价不同。无论是认可中心式数据控制者对数据享有作为绝对权的财产权,还是通过《反不正当竞争法》对数据企业就数据享有的合法利益予以保护,很重要的理由就是数据企业在收集数据时支付了对价,付出了成本。申言之,数据企业本身收集处理个人数据的行为就需要付出相应的成本,且他们向个人数据被收集者支付了合理的对价,符合公平原则,理应产生相应的民事权利。数据企业不可能凭空收集到个人数据,它们需要付出成本来研发各种产品、持续地向用户提供相应的服务,方可在此过程中不断收集个人数据并累积成海量的数据。[26]用户之所以愿意让数据企业收集并使用个人数据,也是因为数据企业提供了免费使用的各种数据产品和软件服务(如人们日常生活中大量使用的各种App)。当然,用户也并非免费使用这些产品或服务,表面上他们虽然未直接付费,但个人数据实际上就是对价,即用户需要同意为其提供产品或服务的企业收集个人数据,并在告知使用目的且不侵害用户既有民事权益的前提下对这些个人数据加以使用。这样一个用户与数据企业合作的模式中,数据企业向用户提供数据产品和服务属于数据企业为个人数据支付的对价。故此,基于公平原则,应当认定数据企业对被合法收集的

个人数据享有权利。

然而，在公共区块链中，任何节点在监听、接收和验证数据有效性的过程中，均不存在对产生区块数据的节点支付对价的行为。对区块数据进行监听、接收和验证数据的一方，并没有义务向广播区块数据的节点支付对价。恰恰相反，由于各个节点对区块数据进行接收和验证的过程是一个消耗电力与算力的工作，因此，区块链的底层技术结构对该工作支付了对价，如比特币区块链技术就赋予那些率先完成区块创建的人一定数量的比特币，把价值作为激励，促使网络用户有动力保证比特币平台的长期成功，购入顶尖装备来挖矿并更高效地花费能量从而维护账本。[27]显然，这与数据控制者向网络用户支付对价的权利义务结构完全不同。

(四)联盟链与私有链中的数据权属

尽管公共区块链的技术特征并没有授予任何节点对区块数据享有数据权益，但联盟链以及作为联盟链特殊形态的私有链，有所不同(参见图1)。就联盟链而言，其节点是事先选择好的，联盟成员之间存在合作关系。因此，其并非完全去中心化，只是部分去中心化。至于私有链，更是将参与的节点限定在有限的范围，写入的权限也完全操控在参与者手中。因此，在联盟链与私有链中，当事人可以约定这两类区块链中数据的归属。具体而言，首先，联盟链中的成员和私有链中的私有用户对于自己上传至区块链上的数据应当享有相应的民事权益。因为，在联盟链和私有链中的这些数据可能是联盟成员自己收集、存储和加工的数据资产，也有可能是联盟成员制作的有关信息资料。就这些数据而言，它们都是联盟成员作为中心式的数据收集者从事合法数据收集处理活动而取得，所以应当承认联盟成员对自己的这些数据享有相应的民事权益。联盟成员可以将这些数据上传至区块链，同时也可以和其他联盟成员来约定这些数据资产的归属。当然，各个联盟成员仅对自己上传至区块链上的数据享有权利，只能授权他人知悉和利用自己享有权利的数据。

其次，联盟链的技术特征允许联盟成员就数据权属进行特别约定。联盟链(Consortium Blockchain)是指参与区块链的节点是事先选择好的，节点间通常有良好的网络连接等合作关系，区块链上的数据可以是公开的也可以是内部的，因此联盟链是部分意义上分布式、“部分去中心化”的区块链。[28]联盟链允许预先约定各个节点对区块链的访问权限，例如，可以允许每个节点可读取或者只受限于共识验证参与者，或走混合型路线如区块的根哈希及应用程序接口对外公开，允许外界用来进行区块链数据和区块链状态信息的查询等。不过，联盟成员对数据权属的特别约定应当满足法律规定，即不得侵害他人商业秘密或隐私。基于联盟链的这一技术特点，各个节点可以在创建基础区块链时就区块数据的权属

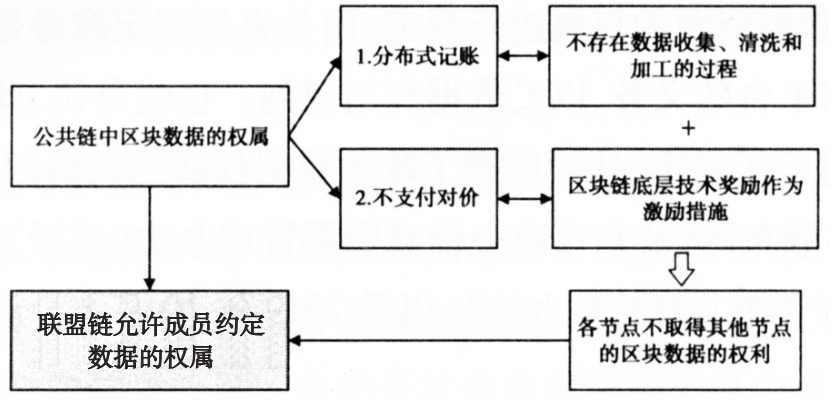

图1 公共链与联盟链的数据权属对比

问题达成协议，如约定某个节点对区块数据享有收集、存储和利用的权利，或某些节点对区块数据只具有访问和查询的权限，但不得利用这些数据资产。

三、区块链中的政务数据权属

随着电子政务建设的不断完善，行政机关在履行职责过程中越来越大量地收集和获取的个人数据，也形成了具有财产价值的数据集合。行政机关依法履行行政职能中收集的数据集合被称为“政务信息资源”“政务数据”或“公共数据”。国务院印发的《政务信息资源共享管理暂行办法》第2条规定，政务信息资源，是指政务部门(即政府部门及法律法规授权具有行政职能的事业单位和社会组织)在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或者通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等。

2019年10月24日下午，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习，习近平总书记在主持本次政治局集体学习时指出：“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，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。”因此，在可预见的将来政务部门将更多地利用联盟链和私有链的方式实现数据的互通共享，政务信息资源在政府部门之间的广泛流动和大量交换将成为现实。故此，有必要明确联盟链和私有链上这些政务数据集合的权属问题。

目前，在法律和行政法规中并未对政务数据资源的权属作出界定。从一些地方性法规和规章来看，对于政务数据资源的归属有两种不同的态度。一种是明确规定政务数据资源属于国家所有。例如，2015年2月15日福建省人民政府通过的《福建省电子政务建设和应用管理办法》第9条规定：“应用单位在履行职责过程中产生的信息资源以及通过特许经营、购买服务等方式开展电子政务建设和应用所产生的信息资源属于国家所有，由同级人民政府电子政务管理部门负责综合管理。”再如，2019年7月31日重庆市人民政府通过的《重庆市政务数据资源管理暂行办法》第4条第1款规定：“政务数据资源属于国家所有。”理论界也有学者认为，应当明确将政务信息资源界定为国家所有，这就意味着政务信息资源属于公共资源，公众可以接近或使用政务信息资源，从而避免政府部门独占该数据资产。[29]

另一种则并未对政务数据资源的权属进行规定，而是直接规定政务数据开放的方法、政府制定开放目录的义务、建设数据平台的义务以及数据利用规则。也就是说，此种模式采取了所谓“责任规则”的方式对政务数据进行了规定，从而回避了政务数据权属的归属问题。采取这种模式的地方立法如2017年12月27日颁布的《北京市政务信息资源管理办法(试行)》，2018年9月4日施行的《宁夏回族自治区政务数据资源共享管理办法》，以及2019年10月1日施行的《上海市公共数据开放暂行办法》。

笔者认为，立法上明确规定政务数据资源属于国家所有，并无不妥。但是，国家取得政务信息资源的所有权，与企业等数据控制者对其所收集、存储的数据资产取得财产权利的原因有所不同。一方面，企业等数据控制者收集个人数据的正当性基础在于获得自然人的同意。行政机关收集政务信息的正当性基础在于行政机关履行法定职责以及行政相对人的法定义务。另一方面，数据控制者获得数据财产权利的原因在于数据控制者合法收集处理数据并支付了合理对价的行为，而行政机关取得政务数据权利的原因是基于公共政策的考虑，将政务信息资源界定为国家所有并且各个行政机关有权利用，将有助于行政机关履行其法定职责，也有利于促进政府各个部门之间的数据共享。

因此，政务信息资源的国家所有权并不取决于行政机关是通过何种方式收集处理这些数据。即便是行政机关委托数据企业进行收集的政务信息，虽然数据企业是真正进行数据采集、数据清洗和加工的主体，但只要该信息属于行政机关履行职责过程中应当获取的信息，那么这些数据企业收集的政务

信息资源也应归国家所有。同样,行政机关采用区块链技术的方式获取政务信息资源,也归国家所有。在这一点上,并不因为区块链技术中不存在一个中心式的数据控制者而有所不同。

当然,政务数据资源归国家所有意味着其不属于任何特定的行政机关等政务部门所有,否则,就会导致一些机关以此为由而拒绝政务数据的互通共享及对外开放。《政务信息资源共享管理暂行办法》第5条明确规定,政务信息资源以共享为原则,不共享为例外。各政务部门形成的政务信息资源原则上应予共享,涉及国家秘密和安全的,按相关法律法规执行。"需求导向,无偿使用。因履行职责需要使用共享信息的部门提出明确的共享需求和信息使用用途,共享信息的产生和提供部门应及时响应并无偿提供共享服务。"[30]

就政务数据资源对公众开放的法律规制问题,目前有两种观点。一种观点认为,面对政务服务对象要求公开、查询、复制相应的政务数据信息时,应当严格遵循《政府信息公开条例》等法律法规的规定,即除非依法确定为国家秘密的政府信息,法律、行政法规禁止公开的政府信息,以及公开后可能危及国家安全、公共安全、经济安全、社会稳定的政府信息,不能公开外,其他的政府信息应当坚持以公开为常态、不公开为例外,遵循公正、公平、合法、便民的原则。[31]此种观点进一步认为,鉴于目前的《政府信息公开条例》的范围过窄,因此有必要对之加以适当的修改,从而将信息公开的范围扩展到政府数据。[32]

另一种观点则认为,政务数据的开放和政府信息公开在制度功能、关系结构等方面均有差异。例如,政府数据开放是要求对底层的、原始的数据加以公开,《政府信息公开条例》中公开的政府信息,则是经过加工和分析的信息,而往往并非原始的数据。[33]再如,在政府数据开放中,政府的角色及其与公众的关系不同于政府信息公开。主动开放是政府数据的基本开放方式,较之信息公开,政府透明度得到进一步提升,更容易在政府与公众之间建立起信任关系,缓和双方之间的对立关系。[34]故此,应当制定《开放政府数据法》或《政务数据开放条例》,专门对于政务数据或政府数据的开放作出规定。

笔者认为,这两种观点本质上并不矛盾,二者都认为政务数据应当开放,从而既保护公众的知情权,改进公共服务和推动创新发展,至于采取单独立法还是修订既有立法,只是立法技术路线上的差异而已。总的来说,行政机关在履行法定职责的过程中,依照法律规定直接或者通过第三方服务所获取和制作的各类政务信息资源,无论是否上传至区块链中,都应当属于国家所有,各个行政机关对此享有依法存储、利用和共享的权力。自然人、法人或者非法人组织则享有依法获取并使用政府数据信息的相应权利。[35]

四、结论

综上所述,应当在区分公有链、联盟链和私有链的基础上分别确定区块链中数据的权属。首先,对于公共区块链而言,任何节点或用户对于区块链上记载的、非自己上传的数据均不享有任何民事权益,否则,将对公共区块链的发展产生严重的法律障碍。其次,在联盟链和私有链中,可以由参与成员对区块数据的权属与利用方式进行约定,但各个成员仅能对自己所有的数据进行约定,且不能违反法律法规,不得侵害他人隐私权、个人信息等。最后,政务机关在履行法定职责的过程中,依照法律规定直接或者通过第三方服务所获取和制作的各类政务信息资源,无论是否上传至区块链中,都应属于国家所有。

致谢:感谢中国人民大学法学院熊丙万副教授、清华大学法学院博士生阮神裕同学提供的帮助!

注释:

①长铗、韩峰等:《区块链:从数字货币到信用社会》,中信出版集团2016年版,第48页。

②华为区块链技术开发团队:《区块链技术及应用》,清华

大学出版社2019年版,第90页。

③[英]罗伯特·赫里安:《批判区块链》,王延川、郭明龙译,上海人民出版社2019年版,第48页。

④[美]凯文·沃巴赫:《链之以法:区块链值得信任吗?》,林少伟译,上海人民出版社2019年版,第13-14页。

⑤2019年10月31日十九届四中全会通过的《中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干重大问题的决定》已明确将数据作为一类重要的资产。

⑥石宏主编:《〈中华人民共和国民法总则〉条文说明、立法理由及相关规定》,北京大学出版社2007年版,第309页。

⑦孔祥俊:《反不正当竞争法新原理·原论》,法律出版社2019年版,第93页。

⑧参见"北京淘友天下技术有限公司、北京淘友天下科技发展有限公司与北京微梦创科网络技术有限公司不正当竞争纠纷案",北京知识产权法院(2016)京73民终588号民事判决书;"武汉元光科技有限公司与深圳市谷米科技有限公司不正当竞争纠纷案",广东省深圳市中级人民法院(2017)粤03民初822号民事判决书;"淘宝(中国)软件有限公司与安徽美景信息科技有限公司不正当竞争纠纷案",杭州市中级人民法院(2018)浙01民终7312号民事判决书;"北京百度网讯科技有限公司与上海杰图软件技术有限公司不正当纠纷案",上海知识产权法院(2016)沪73民终242号民事判决书。

⑨参见 Barbara Anna Radoń, Trade Secrets Protection for "Big Data": Personal Data as Trade Secrets in the European Union, Munich Intellectual Property Law Center Master Thesis (2015/16). Lara Grow & Nathaniel Grow, Protecting Big Data in the Big Leagues: Trade Secrets in Professional Sports, 74 Washington and Lee Law Review,(2017).

⑩程啸:《论大数据时代的个人数据权利》,载《中国社会科学》2018年第3期,第121页。

⑪龙卫球:《数据新型财产权构建及其体系研究》,载《政法论坛》2017年第4期,第75-76页。

⑫ Stuart Banner, American Property: A History of How, Why, and What We Own, Harvard University Press, 2011. at 289.

⑬ Matthias Berberich & Malgorzata Steiner, Blockchain Technology and the GDPR-How to Reconcile Privacy and Distributed Ledgers, 2 Eur. Data Prot. L. Rev.422(2016), at 424.

⑭需要说明的是,区块链上的数据不包括特定数据的哈希校验值。特定数据的哈希校验值是对数据进行密码学加工后形成的数值,而非数据本身。

⑮2018年2月2日,在工业和信息化部信息化和软件服务业司指导、工业和信息化部中国电子技术标准化研究院主办的"中国区块链技术和产业发展论坛第二届开发大会"上,主办方发布了《区块链·数据格式规范》,本文采取的是该规范所确定的区块链上的数据分类方法。

⑯华为区块链技术开发团队:《区块链技术及应用》,清华大学出版社2019年版,第56页。

⑰长铗、韩锋等:《区块链:从数字货币到信用社会》,中信出版集团2016年版,第52页。

⑱长铗、韩锋等:《区块链:从数字货币到信用社会》,中信出版集团2016年版,第53页;华为区块链技术开发团队:《区块链技术及应用》,清华大学出版社2019年版,第59页。

⑲袁勇等:《区块链技术发展现状与展望》,载《自动化学报》2016年第4期,第484页。

⑳[加]唐塔普斯科特、亚历克斯·塔普斯科特:《区块链革命》,凯尔、孙铭、周沁园译,中信出版集团2016年版,第33页。

㉑袁勇等:《区块链技术发展现状与展望》,载《自动化学报》2016年第4期,第486页。

㉒刘智慧、张泉灵:《大数据技术研究综述》,载《浙江大学学报》(工学版)2014年第6期,第962页。

㉓ Nakamoto S., Bitcoin: a peer- to- peer electronic cash system, available: https://bitcoin.org/bitcoin.pdf, 2009.

㉔参见长铗、韩锋等:《区块链:从数字货币到信用社会》,中信出版集团2016年版,第62页。其他的合法性验证即共识算法还包括"权益证明"(proof of stake)"委托股权证明"(Delegated proof of stake)、瑞波共识等。

㉕程啸:《论大数据时代的个人数据权利》,载《中国社会科学》2018年第3期,第118页。

㉖例如,在"北京淘友天下技术有限公司、北京淘友天下科技发展有限公司与北京微梦创科网络技术有限公司不正当竞争纠纷案"中,被侵权人微梦公司之所以能够积累数以亿计的微博用户以及与相关的大量个人数据,就是因为该公司多年来持续经营"新浪微博"这一兼具社交媒体网络平台和向第三方应用提供接口开放平台所致。参见北京知识产权法院(20t6)京73民终588号民事判决书。

㉗[加]唐塔普斯科特、亚历克斯·塔普斯科特:《区块链革命》,凯尔、孙铭、周沁园译,中信出版集团2016年版,第35页。

㉘长铗、韩锋等:《区块链:从数字货币到信用社会》,中信出版集团2016年版,第52页;袁勇等:《区块链技术发展现状与展望》,载《自动化学报》2016年第4期,第490页。

㉙曾娜:《政务信息资源的权属界定研究》,载《时代法学》2018年第4期,第32-33页。

㉚《政务信息资源共享管理暂行办法》第9条将政务信息资源按共享类型分为无条件共享、有条件共享、不予共享等三种类型。其中,可提供给所有政务部门共享使用的政务信息资源属于无条件共享类;可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用的政务信息资源属于有条件共享类;不宜提供给其他政务部门共享使用的政务信息资源属于不予共享类。

㉛例如,《浙江省公共数据和电子政务管理办法》第25条规定:"公共数据资源开放目录外的公共数据开放,应当遵守下列规定:(一)法律、法规规定应当开放的公共数据,开放前应当告知同级公共数据和电子政务主管部门;(二)法律、法规禁止开放的公共数据,不得开放;(三)其他公共数据开放,应当经同级公共数据和电子政务主管部门审核同意。"

㉜肖卫兵:《论我国政府数据开放的立法模式》,载《当代法学》2017年第3期,第47页。

㉝宋华琳:《中国政府数据开放法制的发展与建构》,载《行政法学研究》2018年第2期,第35-46页。

㉞王万华:《论政府数据开放与政府信息公开的关系》,载《财经法学》2020年第1期,第19页。

㉟有观点认为,要区分私人使用政府数据的方式,如直接使用和增值使用、公益性使用和商业性使用分别加以规范。参见:吕富生:《论私人的政府数据使用权》,载《财经法学》2019年第6期,第34页。

On Ownership of Data in the Blockchain

Cheng Xiao

Abstract: The problem concerning the ownership of data in the blockchain refers to the special data of users on the chain, that is, the ownership of transaction data, entity data and contract data, and whether other blockchain users can process and use the data. The ownership of data in the public blockchain, the consortium blockchain, or the private blockchain should be researched separately. In the public blockchain, since there is no centralized data controller or data collection behavior, any node or user does not have any rights of the data recorded on the shared chain and not uploaded by itself. In the consortium blockchain and the private chain, participating members can make special agreements on the ownership of data. Government data on the blockchain should be owned by the state.

Key words: the blockchain; data; ownership; collect; process