法商研究 Studies in Law and Business
Vol. 37 No. 4 (2020)

网络与信息法

区块链类型化的法理解读与规制思路

赵 磊*

摘 要:根据区块链技术内部结构的不同,可将之分为公有链、私有链与联盟链3种类型。公有链是完全去中心化的,参与者之间形成"技术信任"机制;私有链是中心化的,所有参与者完全依赖主导者;联盟链是部分中心化的,参与者通过协议进行合作。公有链通过算法争夺记账权形成共识机制,私有链各个节点的记账权是中心机构赋予的,联盟链的共识机制是各个节点之间的彼此信任。联盟链兼具公有链与私有链的优势,具有信用多元、信息共享与高效率的特点,可广泛应用于社会治理各方面。公有链的发展必须受到严格控制,对私有链要针对其应用领域和法律关系进行监管,对联盟链则应实施穿透式监管。

关键词:区块链 公有链 私有链 联盟链 法律规制

DOI:10.16390/j.cnki.issn1672-0393.2020.04.003

一、引言

2019年10月24日,中共中央政治局就区块链技术发展现状和趋势进行了第十八次集体学习。中共中央总书记习近平强调:"要探索建立适应区块链技术机制的安全保障体系,引导和推动区块链开发者、平台运营者加强行业自律、落实安全责任。要把依法治网落实到区块链管理中,推动区块链安全有序发展。"①

区块链是一种不依赖第三方,通过分布式数据库进行数据存储、验证、传递和交流的技术方案,具有去中心化、集体维护、开放性和时序数据不可篡改等特征。② 正是这些极具颠覆性的技术特征,使得区块链不仅在经济领域具有极大的商业价值,而且可以应用到社会治理的方方面面。随着发展区

* 中国社会科学院法学研究所研究员

基金项目:中国社会科学院重大国情调研项目(GQZD2020007)

① 佚名:《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》,《人民日报》2019年10月26日。

② 参见赵磊:《论区块链技术背景下信用制度的挑战与机遇》,载许多奇主编:《互联网金融法律评论》第9辑,法律出版社2017年版,第38页。

块链产业被上升到国家战略层面，可以预见区块链技术在我国社会各领域的应用必将迎来蓬勃发展的局面。不过，需要注意的是，作为比特币的底层架构，最初的区块链技术是一种“点对点”的信息传输系统，具有全网认证、匿名化以及去中心化等特点，因之而产生运行效率低下、能源消耗量大等问题。更重要的是，比特币这种公有区块链天然排斥监管，引起了各国政府的警惕，在应用场景上受到诸多限制。

为了克服上述弊端，基于商业利用的需求，区块链技术发展出3种类型：公有链、联盟链与私有链。三者的运行机制不同，共识机制与中心化程度也不同。正因为如此，建基于虚拟世界，起源于数字货币，力图构建去中心化结构的区块链技术，由于内外的种种原因，逐渐向现实世界回归，开始在连接虚拟世界与现实世界的过程中，展现出更广阔的前景和价值。① 为了保障区块链产业安全有序发展，必须结合应用场景，选择合适的区块链类型，并对其进行有针对性的监管与规制。

二、公有链：区块链的最初形态

（一）区块链的技术特征及其运行机制

作为区块链技术的最初应用形态，比特币是“一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构”。②可以说，中本聪发明比特币的动机就是要去中介化、去中心化，实现在交易双方之间的“点对点”（peer to peer）支付。比特币的协议和软件都是公开发布的，世界各地的任何开发人员都可以查看其代码，或者开发他们自己修改过的比特币软件版本。没有谁拥有比特币网络，就像没有人拥有电子邮件背后的技术一样。比特币由世界各地所有的比特币用户控制。

可见，最早的区块链是一个完全开放的系统，不由任何个人、组织或机构控制，而是由所有参与主体共同维护，这就是所谓公有链（public blockchain）。公有链对世界上所有人开放，用户不需要注册和授权就能够匿名访问网络和区块，参与记账和交易，并且可以自由加入和退出网络。任何人都可以参与共识过程——决定添加何种区块到链上并确定其内容。公有链之所以可以做到上述几点，是因为其有以下几方面的技术支撑和机制设计：

1. “点对点”网络技术。点对点网络技术是一种无须中央服务器，用户群通过互联网连接、彼此交换信息而存在的分布式网络架构。用户加入系统的唯一要求是其电脑终端连接因特网和P2P软件，这使每个用户可以访问网络上成千上万的其他节点。点对点的信息传递，使得第三方信用中介成为多余，交易在双方当事人之间完成，简化了程序、压缩了成本。每一个节点都参与所有交易信息的验证，一方面起到见证的作用；另一方面使得信息不能被篡改。

2. 非对称加密技术。点对点技术在传递信息时，既要让全网获知，又要保护交易双方当事人的隐私，这是应用非对称加密技术实现的。非对称加密技术包含两个密钥，一个是公钥（public key），另一个是密钥（private key）。公钥用于对信息加密且是公开的，所有参与者可见；私钥用于解密，只有信息的拥有者才有权用其解密。因为私钥与公钥不同，因此被称为非对称加密。非对称加密技术算法复杂、安全性强。通过综合运用该技术与点对点网络技术，可以建立分布式交易账簿，并以呼叫问

① 参见肖风：《从公有链到私有链：区块链回归现实》，《当代金融家》2016年第2期。

② 中本聪：《比特币：一种点对点的电子现金系统》，https://nakamotoinstitute.org/static/docs/bitcoin－zh－cn.pdf，2019－12－02。

答机制向全网广播,网络节点不停地检查接收的数据,避免数据被篡改。①

3. 时间戳(time stamp)与哈希现金(Hash Cash)算法。中本聪设计比特币遇到的最大难题是如何解决双重支付(double spend)问题,他的方案是通过区块链全网记账的方式,替代了第三方信用机构。服务器通过对以区块形式存在的一组数据实施随机散列而加上时间戳,并将该随机散列进行广播,该时间戳能够证实特定数据于某特定时间是的确存在的,因为只有在该时刻存在才能获取相应的随机散列值。每个时间戳应当将前一个时间戳纳入其随机散列值中,每一个随后的时间戳都对之前的一个时间戳进行增强,这样就形成一个链条,每个区块都包含上一个区块的哈希值,区块之间的衔接也是通过哈希算法完成的。随机散列值及其运算方法就是哈希现金算法。②

4. 共识机制。区块链技术是去信任、去信用的系统。这是因为,区块链建立了共识机制,即在一个互不信任的市场中,要想使各节点达成一致的充分必要条件是每个节点出于对自身利益最大化的考虑,都会自发、诚实地遵守协议中预先设定的规则。判断每一笔记录的真实性,最终将判断为真的记录记入区块链之中。③ 这些需要通过哈希算法来完成,当某个节点得到合理的哈希值时,也就说明其进行了大量计算,对其计算工作给予的奖励,就是所谓“工作量证明”(Proof of Work)。只要某个节点耗费的工作量能够满足该工作量证明机制,那么除非重新完成相当的工作量,该区块的信息就不可更改。由于之后的区块是链接在该区块之后的,因此想要更改该区块中的信息,就需要重新完成之后所有区块的全部工作量。在节点足够多且无中心控制的情况下,对区块链信息的篡改几乎是不可能完成的任务。比特币的工作量证明是“挖矿”——某个节点计算随机散列数据的过程,完成后形成一个区块,并对其奖励一定数额的比特币。

(二)技术信任而非制度信任:区块链的最大价值

通过上述应用技术和合理机制的安排,区块链技术解决了人们交往与合作中的信任问题。在陌生人社会,人与人之间缺乏了解、信息不对称,市场交易始终处于一种不完全的信息状态,人们基于对他人“机会主义行为”以及未来不确定性的担忧,往往需要建立各种纷繁复杂的担保法律制度,以确保交易安全。在区块链系统中,点对点信息传递、分布式记账以及非对称加密等技术的应用,实现了信息的真实化、透明化以及不可篡改,解决了困扰人类社会几千年的信任问题。

从信任的角度来看,区块链实际上是用数学方法解决信任问题的产物。过去社会的有效运行主要靠法律制度建立规则,进而形成信任来规范和引导社会成员的行为。区块链技术的出现和运用则是基于共识的数学方法,在机器之间建立信任并完成信用创造。通过非对称密钥解决所有权信任问题,基于区块链的技术优势保证价值转移过程的安全信任,通过智能合约解决信任执行问题,最终实现“无需信任的信任”。④ 从这个意义上说,区块链系统构建的信任机制是对密码学、算法等技术的信任,而非对任何人、组织和制度的信任。

去中心化、去中介化的区块链给交易至少带来以下几方面的好处:一是中间环节减少,节省交易成本。不仅参与方减少,节省开支,而且信息传递更为直接、快速,节省时间成本;二是交易当事人之

① 参见长铗等:《区块链:从数字货币到信用社会》,中信出版社 2016 年版,第 7 页。

② 区块链通常使用 SHA-256(安全散列算法)进行区块加密,这种算法的输入长度为 256 位,输出的是一串长度为 32 字节的随机散列数据。哈希算法对一个交易区块中的交易信息进行加密,并把信息压缩成由一串数字和字母组成的散列字符串。

③ 参见唐文剑、吕雯等编著:《区块链将如何重新定义世界》,机械工业出版社 2016 年版,第 72 页。

④ 唐文剑、吕雯等编著:《区块链将如何重新定义世界》,机械工业出版社 2016 年版,第 37 页。

间信息对称，保障了交易安全。通过分布式记账技术，使得交易信息完全透明，不确定性降低、机会主义行为减少；三是激励机制合理，可以优化资源配置。区块链的工作量证明机制，真正实现了“多劳多得”“不劳不得”，有助于调动参与者的积极性，合理利用资源。

从某种意义上说，区块链的最大价值还不在技术层面，而在于其去中心化、技术信任等特点带给社会生活的促进与启发。如果将之运用到金融、法律与物流等领域，可能会极大提高生产力，带来行业革命；如果将之运用到社会治理的其他方面，可能会大幅推进社会治理体系和治理能力的现代化。

（三）公有链技术的弊端

作为对外开放、去中心化的系统，公有链技术在具有巨大价值的同时，从不同的立场与角度观察，其也存在一些与生俱来、难以克服的弊端：

1.单笔交易效率较低。公有链由于每笔交易都需要向全网广播，所有节点均参与记账，参与者越多，程序就越复杂，耗时就越长。以比特币为例，当有新的交易请求出现时，系统就会在全球范围内自动按一定概率随机选择一个记账人，让其验证这笔交易并记账，然后把更新的账本广播给其他记账人。单笔交易耗时大约 10 分钟左右，所有节点同步数据则需要更多的时间。因此，公有链无论应用到何种场景，其“点对点”“分布式存储”的特性都会导致交易耗时过长的问题。

2.消耗大量能源。因为每笔交易需要整个系统的所有节点参与，需要许多电脑终端进行大量的计算才可以完成，这势必会消耗大量的电能。比特币挖矿就是一项耗电量巨大的公有链交易。据统计，2017 年 11 月，比特币挖矿消耗的电力超过 159 个国家的耗电量，其中包括爱尔兰和非洲大多数国家。截至 2018 年 3 月，该数字已变为 173，这意味着如果把比特币挖矿活动视为一个国家的话，它将成为世界上排第 47 位的电力消费国（略低于科威特，但超过希腊）。①

3.商业应用较为困难。商业活动的目的是追逐经济利益，一般依赖公司这样的经济组织通过资源交换的利差实现经营目的。公有链并无一个中心化的机构，其激励机制是对某个节点工作量提供证明，并不能实现参与者的商业目的。例如比特币挖矿取得一定数量的比特币，是对其工作的奖励，并不是该用户通过交换而取得收益。在二级市场买卖比特币获取的收益，并不是比特币区块链本身产生的收益。这使得公有链很难找到合适的商业应用场景。而且，基于工作量证明机制的挖矿行为还造成了大量的资源浪费，达成共识所需要的周期也较长，因此该机制并不适合商业应用。② 这种依靠消耗大量能源完成区块链共识机制的模式，被认为是不可持续的。③

4.难以被监管。公有链去中心化的特点与无政府主义契合，天然排斥监管。作为公有链最初应用形态的比特币，不是由任何国家或地区政府发行的，并无政府信用为其背书，但仍然在全世界受到许多人欢迎和追捧。这一方面是因为其存在一定的利用价值，另一方面也说明很多人信奉去国家、去政府的观念。早在 20 世纪 70 年代，哈耶克就提出货币不应该被政府所垄断，每个人、组织都有权发行货币，参与货币市场的竞争。④ 这种思想与比特币产生之间的因果关系不得而知，但其对区块链技

① See Estimated Electricity Cost Of Mining One Bitcoin By Country, https://powercompare.co.uk/bitcoin-electricity-cost/, 2019-12-28.

② 参见唐文剑、吕雯等编著：《区块链将如何重新定义世界》，机械工业出版社 2016 年版，第 73 页。

③ 参见[加]唐·塔普斯特、[加]亚力克斯·塔普斯科特：《区块链革命：比特币底层技术如何改变货币、商业和世界》，凯尔等译，中信出版社 2018 年版，第 243 页。

④ 参见[英]弗里德里希·冯·哈耶克：《货币的非国家化——对多元货币的理论与实践的分析》，姚中秋译，新星出版社 2007 年版，第 186～190 页。

术的发展影响深远。公有链的用户通过互联网连接,可能分散在世界任何一个角落,某一国或地区的政府无法对全网进行监管。

三、私有链的运行机制

公有链技术的弊端是自身无法克服的,根本原因在于其与生俱来的去中心化特点,这使得其商业应用受到很大限制。为此,一些商业组织尝试对公有链进行改造,私有区块链(以下简称私有链)应运而生。

(一)私有链是中心化的分布式存储数据库

所谓私有链(private blockchain),是指系统的写入权限与读取权限是否对外开放、开放程度如何以及受到何种程度的限制均受到某一组织或机构控制的区块链。私有链颠覆了公有链的去中心化特征,背离了区块链技术的初衷。大多数人一开始很难理解私有链存在的必要性,认为其与中心化数据库没太大区别,甚至还不如中心化数据库的效率高。对此,有学者认为,事实上,中心化与去中心化永远是相对的,私有链可以看作是一个小范围系统内部的公有链,如果从系统外部来观察,这个系统可能仍是中心化的;但从系统内部每一个节点的角度来看,当中每个节点的权利又是去中心化的。[①] 这种说法固然有一定的合理性,但存在对中心化含义的误读。区块链去中心化的特点是就整个系统而言的,并不是指每个节点自身。何况在系统完全中心化的前提下,每个节点的权利与义务是完全不由自己掌握的。在一个私有链中,中心化的所有者可以是单个公司或其他组织。让谁加入区块链系统、赋予其多大的读写权限,均由该中心化组织决定。他们甚至可以根据需要覆盖或删除区块链上的任何信息。这也是该组织将区块链系统设置为中心化的初衷和主要原因。从这个意义上说,私有链本质上是一种特殊的分布式存储数据库。

(二)私有链的共识机制较弱

区块链的共识机制是为了解决信任问题而设计的。在无中心化机构的公有链系统中,共识机制一般是工作量证明,共识机制是在所有参与者均有记账权的前提下通过非对称加密算法而形成。通常,公有链会用某种代币(token)作为工作量证明的符号象征,以奖励那些参与记账的节点。私有链节点的记账权是中心化机构赋予的,如何记、记多少均非节点主动所为,在系统内难以形成价值共识。因此,在私有链系统中,也无须设计代币激励机制。

2019 年 4 月,全球知名评级机构穆迪发布了一份区块链在证券领域应用的报告,详细分析了区块链技术对金融公司的利弊。报告认为私有链和公有链在安全方面存在一定差异,并表示私有链中的共识机制可能没有公有链的共识机制那么强,有的私有链甚至可能完全没有共识机制。[②] 在缺乏明确共识机制的前提下,私有链通过中心化机构预先设定的智能合约运行。私有链的智能合约无非是中心化机构根据该私有链的工作目的需要,设计一组复杂的、带有触发条件的数字化承诺,该合约能够按照主导者的意志自动正确执行。除主导者以外,其他节点不能对链上信息做任何修改,因而也具有一定程度的自动执行和不可篡改性。由于缺乏确定的共识机制,公有链的工作量证明方式也不能适用于私有链。私有链上各个节点的激励机制完全依赖于主导者的预先设定和安排,并且随时可

① 参见龚鸣:《区块链社会:解码区块链全球应用与投资案例》,中信出版社 2016 年版,第 22 页。

② See Blockchain Improves Operational Efficiency for Securitisations, Amid New Risks, Structured Finance, Moody's Investors Service, 25 April 2019, p.9.

能会被调整。

（三）私有链的技术特征

与公有链相比，私有链牺牲了区块链技术的去中心化，整个系统由中心化的机构设计、控制，这使得私有链具有以下几个方面的特征：

1.私有链是封闭的区块链系统。私有链利用了区块链的分布式存储、智能合约等技术，但并不是向社会开放的网络系统。任何参与者的加入都来自主导者的邀请或同意，且必须经过身份验证。链上各个节点一般实名参与，便于身份的准确识别。这决定了私有链通常被用于相对封闭的场景，如企业内部管理中，为了搜集、存储和整理各个流程、不同区域的数据，建立私有链系统；某个金融类企业对自己的业务流程进行管理，等等。

2.私有链效率高、成本低。与公有链需要花费很长时间达成共识不同，私有链的交易信息无须所有节点进行验证，数据管理和信息交换工作由系统设定的个别节点或者中央处理节点完成。单位时间内，私有链系统处理的交易量更大，速度更快，运行的效率大为提高。同时，这也大大降低了系统内部各个节点的交易成本以及系统运行的总成本。

3.私有链相对安全。公有链是开放式平台，任何人都可自由加入或退出。除非达到类似于比特币这样的规模，公有链在信息安全上存在一定的风险。私有链因其中心化、封闭性的特点，为用户提供了一个相对安全、可追溯、不可篡改、自动执行的运算平台，可以防范来自内部和外部对数据的攻击或篡改。私有链上访问权限被严格控制在系统内并由主导者预先设定，在没有权限的情况下，任何人无法获得区块链上的数据和信息。这对公有链系统来说，是几乎不可能做到的。

当然，私有链的中心化特征与区块链技术的初衷相背离，极易成为被某个机构或组织控制的内部系统，引发机会主义和代理成本。这正如穆迪报告中所提到的那样："私有（中心化）链更容易受到欺诈风险的影响，因为其系统设计和治理集中在一方或几方手上。这是区块链治理时风险控制的关键问题。在这种情况下，只有那些治理结构和责任分配制度更加清晰的私有链才是真正的赢家。此外，虽然去中心化系统让数据恢复和审计更容易，但是却引发了更多网关攻击事件。"①

四、联盟链的运行机制

联盟链是指其共识过程受到预选节点控制的区块链，只针对特定某个群体的成员和有限的第三方，内部指定多个预选的节点为记账人，每个区块的生成由所有的预选节点共同决定。联盟链涉及介于公有链和私有链之间的区块链技术，被认为是半去中心化（semi－decentralized）区块链。联盟链背后的主要思想是利用区块链技术创建一个有利的网络，通过扩大合作效果来应对特定行业的挑战。该网络不仅包括业务盟友，甚至还包括竞争对手。德勤会计师事务所的研究表明，74％的组织正在与竞争对手一起参加联盟链或有意愿加入其中。②

（一）联盟链是部分去中心化的区块链

联盟链是对公有链和私有链取长补短而产生的，为了满足多方参与者平等合作而不能由某一方

① Blockchain Improves Operational Efficiency for Securitisations, Amid New Risks, Structured Finance, Moody's Investors Service, 25 April 2019, p.11.

② See Deny, How the Consortium Blockchain Works, September 25, 2019, https://blockchain.intellectsoft.net/blog/how－the－consortium－blockchain－works/, 2019－12－25.

独家掌控的需求,联盟链舍弃了公有链的完全去中心化与私有链的单一中心化,转而采用部分去中心化(也称为半去中心化)的结构。

区块链作为一种共识机制,去中心化的意义就是没有一个组织或个人对全链信息的真实性与完整性承担责任。也正因为如此,所有参与者基于对技术与规则的信任达成共识,相信没有任何一个人可以控制区块链,不会对链上的信息进行篡改。① 这是公有链技术的核心价值。如前所述,作为中心化的私有链,其存在价值主要是基于内部管理的需要,利用区块链技术保证系统内信息的完整准确与不可篡改。联盟链的部分去中心化试图综合两者的技术优势。一方面联盟链并无中心化的主导者,而是由多个节点共同维护的系统。各个节点之间地位平等,彼此之间并无支配关系。系统运行规则由参与各方共同制定,共同遵守。从这个意义上说,联盟链是去中心化的。另一方面,与公有链不同,联盟链严格限定参与者范围,是一个封闭的系统,任何节点的加入和退出必须符合实现预定的规则或者经过其他节点同意。各个节点分别连接不同的参与者,每个节点可以在自己内部建立相对独立的数据库。从这个意义上说,联盟链是多中心化的。因此,联盟链通常被认为是部分中心化(或半中心化)的区块链技术。

(二)联盟链的共识机制

公有链是对外完全开放的,任何人可以随意进出,由于参与者之间互不相识,缺乏信任基础,在没有中心化机构的前提下,必须依赖共识机制代币进行激励。因此,公有链通过工作量证明机制,需要参与者利用极高硬件要求的终端进行复杂的计算,并且花费一定的时间、消耗相当多的电力进行 SHA256 运算,来争夺记账权,代币是其记账权的表现形式。

与公有链相比,联盟链是相对封闭的,参与者之间彼此熟知,有一定的信任基础,共识机制的建立无须通过工作量证明的方式达成。同时,因为并无一个绝对中心化、权威的参与者,还需要在参与者之间形成必要的共识。这决定了联盟链的共识机制必须体现所有参与者的意志,由他们共同磋商完成。对此,既可以在系统成立前预先设定,也可以在系统运行过程中随时调整。如果说,公有链是“信任机器”,必须通过一定的运算才能形成共识,是一个线上的技术问题;那么,联盟链则是“信任人”(人与人之间、人与组织之间,或者组织与组织之间),并非技术问题,无须经过计算来完成,而是一个线下的磋商过程。联盟链的共识机制一旦达成,在智能合约的保证下,程序会自动运行,无须担心数据安全问题。

当然,在联盟链的发展过程中,有些应用场景中也发展出一些特殊的共识机制,以便节省谈判成本,提高系统的运行效率。如 Raft 共识算法在联盟链中的应用,将节点分为候选人(candidate)、领导(leader)和追随者(follower)等角色,在虚拟空间实现了合理的系统治理结构。②

(三)联盟链的技术特征

联盟链是介于公有链与私有链之间的技术,兼具两者的特点。

1.联盟链是相对封闭的系统。联盟链的各个节点都是预先设定的,一般情况下并不对外开放。在特定情况下,根据联盟协议,这种类型的区块链可以允许某些参与者访问或采用混合访问方法,以实现数据共享与数据流通。例如,根哈希(root hash)及其应用程序接口(应用程序接口)可以向公众

① 参见赵磊:《区块链如何监管:应用场景与技术标准》,《中国法律评论》2018 年第 6 期。

② See Diego Ongaro and John Ousterhout, In Search of an Understandable Consensus Algorithm, Open Access to the Proceedings of USENIX ATC '14: 2014 USENIX Annual Technical Conference, pp.307－308.

开放。因此，外部人员或组织可以使用应用程序接口进行一定数量的查询，并获取相关信息。有的联盟链技术甚至在限定一定条件的前提下，完全对外开放。例如，Linux 基金会推出的超级账本架构（Hyperledger Fabric），意在建立一个开源商业联盟链项目，目的是帮助企业建立领先的开源、通用区块链技术结构。超级账本架构目前成员已经超过 250 家机构，既包括 IBM、英特尔、华为等 IT 巨头，也包括荷兰银行、招商银行、中国民生银行等金融机构，还包括耶鲁大学、剑桥大学、北京大学等著名高等院校。①

2.联盟链的参与各方相对独立，但合作紧密。联盟链通常基于业务合作的需求，由多个参与者共同完成。每个参与者通过一个节点接入联盟链，彼此都是不同于其他节点的独立数据库，这既体现了联盟链平等参与、民主管理的特点，又可以最大限度地减少虚拟空间的代理成本和道德风险。公有链参与者之间的“无组织”和私有链参与者之间“被管理”的问题在联盟链中得到了解决，参与者们既保持相对独立，又可以进行紧密合作，非常适合在一些需要数据交换、数据共享的商业场景下应用。因此，一个技术架构较为合理的联盟链会吸引众多参与者加入。

3.联盟链是“不可能三角”的平衡点。国内最早的区块链资讯社区门户网站巴比特的创始人长铗，曾提出区块链技术的三元悖论：去中心化、安全与环保构成了一个不可能三角形，大意是在一个区块链系统中此三者不可能同时实现。② 他所说的环保是指公有链工作量证明需要大量的算力，验证速度慢，耗时较长，实际上是效率问题。因此，区块链技术的不可能三角指的是去中心化、安全与效率三者不可能同时实现。公有链解决了去中心化和安全问题，却牺牲了效率；私有链解决了安全与效率，却牺牲了区块链最具价值的去中心化。从技术原理上来看，联盟链虽然不能完全解决这一问题，但在三者之间找到了较为理想的平衡点。这使得联盟链的参与节点间的连接状态较好、验证效率较高，只需较低的成本即可维持运行，提供高速交易处理的同时降低交易费用，有很好的扩展性，数据也可以保持一定的隐私性。③ 联盟链的运行效率也大大高于公有链。公有链的新区块能否上链，必须由链上的所有节点决定和确认，而联盟链只需要其中几个权重较高的节点进行确定即可。

4.联盟链的数据信息并非不可篡改。在公有链中，除非算力过半，否则数据不可篡改。这是公有链的主要特点之一，是由其“点对点”技术和“去中心化”特征决定的。对联盟链来说，因为其并不是完全去中心化的，如果联盟内部参与者达成合谋，链上的数据仍可以被任意篡改，外部参与者和监管机构无法确认联盟链数据的真实性。

五、区块链技术的分类规制

区块链技术产生十余年来，除了在数字货币领域以外，并未得到广泛应用，其中的根本问题在于如何将这一存在于虚拟空间的技术与现实物理世界相结合，找到合适的应用场景。针对不同的现实需求，运用与之契合的不同类型区块链技术，日益成为区块链产业界的共识。区块链产业发展的规范化、合法化，必须针对不同类型的区块链技术，从制度构建、政府监管以及行业自律几个方面同时进行。

（一）区块链类型化路径的逻辑

① See https://www.hyperledger.org/members，2019－12－20.

② 参见长铗：《不可能三角形：安全，环保，去中心化》，https://www.8btc.com/article/7836，2019－12－30。

③ 参见长铗等：《区块链：从数字货币到信用社会》，中信出版社 2016 年版，第 53 页。

从区块链技术类型出现的先后顺序来看,其经历了从公有链到私有链,再到联盟链的过程。这实际上遵循了从去中心化到中心化,再到部分中心化的路径,这背后的逻辑是商业实践需求。作为最早的区块链应用,比特币出现的前几年,因其规模较小、参与人数少以及技术特征并不明显等特点,并未受到商业界的重视,甚至在技术界的影响也并不太大。随着参与者越来越多,为比特币买卖提供交易平台的数字货币交易所开始涌现。不过,投资比特币这类风险较大的数字货币毕竟只是少数人。公有链去中心化的特点也导致其很难被大规模商业应用,一些有识之士开始尝试挖掘比特币背后的支撑性技术应用到其他领域的可能性。当然,个别基于公有链技术的系统,除了数字货币自身以外,也尝试进入传统商业领域。例如,瑞波系统(Ripple),其基本功能是利用区块链技术在全球范围内建立一个分布式的清算系统,解决跨境的支付清算问题。同时,瑞波系统还可以发行自己的基础数字货币——瑞波币(RXP)。

2015 年 10 月,《经济学人》杂志刊发封面文章,将区块链称为"信任机器",高度肯定了区块链技术在信息传递和价值传输方面的价值。文章称:"比特币的阴暗形象使人们忽视了支撑其底层技术区块链的巨大潜力。这项创新的意义远远超出了加密货币。区块链可以让相互并不信任的人们进行协作,而不必经过中立的中央机构。简而言之,它是一种建立信任的机器。"[①]这引发了很多人的兴趣,特别是一些金融机构,开始尝试将这一技术应用到传统金融业务中去。

银行家们喜欢安全性、零摩擦及即时交易的概念,但他们在开放性、去中心化及新式货币的概念面前退缩了。金融服务业重新打造并私有化区块链技术,将其与一个需要银行或金融机构授权的完全封闭系统结合起来。对他们而言,区块链是一种对关键利益相关者(买家、卖家、托管人与监管者)保持共享及不可擦除记录的数据库,它能够降低成本、降低结算风险及消除故障中心点。[②] 但在实验区块链技术的过程中,鉴于现实世界的法律合规性要求,尤其是政府对持牌金融机构的了解客户及反洗钱方面的严格要求,比特币那样的透明、共享的公有链,不能完全满足持牌金融机构或者其他一些中心化机构的合规要求。[③] 中心化、封闭性强的区块链技术的应用——私有链——应运而生。

人们很快发现写入权限掌握在某个组织或机构手上的私有链技术,可以一定程度上提高单个组织的数据管理水平,但这充其量只是传统数据库的革新,在与外部信息的共享和传输方面,并无太大实际意义。如果借助区块链技术在不同组织之间实现信息共享,必须搭建一条无绝对中心化、各方平等参与的区块链——联盟链。例如,全球顶级区块链联盟 R3,就是通过与来自私营和公共部门的多个行业的 300 多名成员共同开发开源区块链平台 Corda 进行商业合作。[④] R3 的业务范围既包括资本市场、保险、能源等传统商业领域,也包括数字资产、数字身份认证、供应链等新技术领域。目前,我国的平安集团、民生银行、招商银行和中国信息通信研究院等机构已经加入该联盟。

从区块链技术的演进路径可以看出,公有链技术最初出现的原因在于比特币的发明者及其参与者对中心化机构的厌弃,通过互联网技术"点对点"传输信息,追求无约束、无监管的自由,体现的是一种非国家化、无政府主义的私人合作方式。这种理想化的技术显然不能被各国政府接受,在大多数商

① The Trust Machine: The Technology Behind Bitcoin Could Transform how the Economy Works, The Economist, Oct 31st 2015.

② 参见[加]唐·塔普斯特、[加]亚力克斯·塔普斯科特:《区块链革命:比特币底层技术如何改变货币、商业和世界》,凯尔等译,中信出版社 2018 年版,第 8~9 页。

③ 参见肖风:《从公有链到私有链:区块链回归现实》,《当代金融家》2016 年第 2 期。

④ See https://www.r3.com/about/,2019-12-25.

业领域应用的空间也很小。中心化的私有链技术有利于提高单个组织的信息管理水平和保障信息真实安全度，有广泛的应用空间。私有链技术局限于某个组织的内部，在不同组织和机构的合作场景下，如进行信息共享、信息传输，部分中心化、相对开放的联盟链才是最好的选择。从全世界范围来看，区块链技术是互联网领域近年来最大的技术革命，其推崇的“去中心化”“信任机器”“共识机制”等理念令人振奋，但必须结合现实找到适合的应用场景，其技术优势才能够发挥出来。公有链、私有链与联盟链的出现，体现了区块链技术从理想到现实的发展路径。

从应用的角度来看，公有链因为没有一个中心化的机构，外界无法获取链内的任何信息，无法进行监管。我们可以在一些领域发展公有链以参与国际竞争，但必须严格控制其范围。私有链属于某个组织或机构内部的数据管理问题，其应用范围有限。联盟链的多中心化特点，兼顾公有链与私有链的优势，同时又不排斥监管。多中心化的联盟链兼具信用多元、信息共享与高效率的优点，可广泛应用于社会治理各方面。①

（二）严格监管公有链

作为最早的区块链应用，比特币系统是典型的公有链，其作为一种开源的 P2P 软件受到一批技术狂热分子的追捧，有人将其作为一种特殊的投资产品，或是绕过一国政府外汇管制跨境支付的工具。更有甚者，一些个人或机构开始利用比特币从事毒品、走私交易等犯罪活动，如臭名昭著的丝绸之路网站。这引发了各国政府的警觉，开始关注并探讨对比特币等数字货币如何进行监管的问题。

对延伸到公有链技术的其他应用来说，监管问题更是非常困难。主要原因在于公有链技术去中心化的“点对点”分布式架构，导致无法明确地确定监管对象。这一问题并非区块链技术产生后才出现的。20 世纪 90 年代互联网刚刚开始盛行时，主流观点就已经将互联网视为一种以去中心化方式破坏监管的科技。互联网与法律框架之间的持续紧张关系，很大程度上是由参与者“点对点”的分布造成的。② 不过，传统互联网用户虽然可能散乱分布在世界的各个角落，但任何一个终端传输信息必须通过超文本传输协议（HTTP），发送请求到 TCP/IP，再接入到某个中央服务器。每个用户的信息都完整地被存储在某个网站的中央服务器中，监管部门通过对中央服务器的监控，可以准确锁定任一用户。而公共区块链技术并无中央处理器存在，每个节点客户端与服务器端融为一体。用户之间发送信息也不采用传统互联网模式，而是相互验证、分布式存储方式。同时，通过三项加密技术即哈希、公钥/私钥验证和数字签名解决信息安全和隐私问题。这就使得监管部门无法通过某个机构或者组织控制的中央服务器，实现对公有链用户的监管，甚至连用户是谁都无法掌握。

当然，即使如此并不意味着对公有链技术的发展，政府就束手无策了。监管机关虽然无法对具体用户进行监管，但可以对公有链技术的应用和形式进行法律规制和特殊方式的监管。公有链的运行是有特定的算法支撑的，一般包括哈希算法、非对称加密算法以及共识算法。这些算法是由特定的计算机编程代码构成的。这既增加了审查和干预的难度，同时也为恐怖融资和勒索软件提供了便利。另外，在去中心化的区块链系统中，代码也为窃贼创造了一个诱人目标。这是比特币产生以来，区块链技术面临的最突出法律问题。③ 因此，对公有链技术中的算法有必要进行严格监管。从现行法律制度框架来看，对公有链的算法进行监管可以从以下两个方面入手：（1）从密码学角度进行监管。密

① 参见赵磊：《把依法治网落实到区块链管理中》，《光明日报》2019 年 12 月 20 日。

② See Jonathan Zittrain, Internet Points of Control, 44 Boston College Law Review, 687 (2003).

③ 参见[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 61 页。

码学原理是区块链技术的主要支撑,不仅涉及当事人隐私,还涉及数据安全。《中华人民共和国密码法》(以下简称《密码法》)已于 2020 年 1 月 1 日开始实施,其关于商用密码的规定适用于区块链的监管。《密码法》规定了商业密码的行政管理、行业自律以及法律救济等内容,都应该成为区块链密码监管的行为规范。(2)从合同法的角度规范智能合约的运行。智能合约既是区块链决策自动化的算法,也是可以在区块链技术平台上广泛应用的计算机编程代码。智能合约与传统合同既有联系又有区别。两者的联系是智能合约也涉及当事人权利义务关系,只不过是以计算机语言方式在区块链系统中运行。两者的区别在于,智能合约的订立、存储与执行都脱离当事人的主观意志,条件达成自动实现。智能合约对传统合同的挑战,应该纳入现行合同法框架下进行处理。

数字资产是互联网时代的新兴产物,是指那些以电子数据形式存在的具有财产属性与价值的非货币财产,如邮箱、社交账号、网上商城店铺,等等。数字资产的确权一直是法理和实践中的难题。公有链技术的工作量证明机制,根据每个节点的贡献予以相应的奖励,很好地解决了这一问题,如比特币的挖矿就是比特币这一数字资产的原始取得方式。不过,区块链数字资产确权与首次代币发行是两回事,包括比特币在内的绝大多数数字货币并非依靠国家信用做背书的法定货币,迄今为止并无一国政府承认其法定货币地位,也没有任何一国政府公开承认首次代币发行的合法地位。有些国家如日本,在一定范围内承认数字货币具有支付结算功能,并且允许符合资质要求的数字货币交易所运行;美国政府和法院都认为比特币等数字货币不是法定货币,也不是证券,但认为用于项目融资的代币在某种程度上属于证券,应该将其作为证券进行监管。① 中国政府一直对数字货币持非常谨慎的态度,2017 年 9 月 4 日,中国人民银行、中央网络安全和信息化委员会办公室等七部委发布《关于防范代币发行融资风险的公告》,严厉禁止首次代币发行和数字货币交易。

在公有链技术的应用中,应该将数字货币和区块链通证这类区块链资产区分开来,禁止发行和流通那些没有实体项目支撑的数字货币。而对用于实体项目融资的通证这类区块链资产应该承认其合法地位,在不扰乱金融秩序或违反其他法律法规(如危害网络安全或其他财产安全)的情况下,没有否定其存在的必要和理由。② 此外,政府应该制定公有链的技术标准,以去伪存真,同时积极参与区块链技术国际标准的制定,争取国际话语权。

(三)针对私有链的应用领域进行规制

私有链放弃了去中心化这一区块链技术的最大价值,以换取系统运行的高效与安全,适合用于单个组织进行内部业务的信息管理。对此,很多人质疑私有链不过是一种利用分布式账本技术的特殊数据库,许多业内专家认为私有链因为要依托第三方机构(即管理区块链的公司),一般应用于私人企业中,用处不大;还有人认为私有链能解决比特币无法解决的金融企业遇到的问题,如遵守规则制度。③ 因此,私有链广泛应用的空间并不大,组织内部应用私有链技术也与外界无关,无太大必要对其专门进行监管。国家互联网信息办公室 2019 年 1 月 10 日公布《区块链信息服务管理规定》(以下简称《管理规定》),意在规范区块链信息服务活动。《管理规定》第 2 条第 1 款规定:“在中华人民共和

① See Jay Clayton, Statement on Cryptocurrencies and Initial Coin Offerings, Dec. 11, 2017, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11, 2019-12-30.

② 参见长铗等:《区块链:从数字货币到信用社会》,中信出版社 2016 年版,第 222 页。

③ 参见佚名:《专家们分析:私有链的使用案例有哪些?》,https://www.sohu.com/a/366108301_120368953?scm=1002.580041.1040132.PC_ARTICLE_FOCUS&_f=index_pagefocus_4&spm=smpc.content.pic-group.1.1578808489719ntV62HG,2020-01-10。

国境内从事区块链信息服务，应当遵守本规定。法律、行政法规另有规定的，遵照其规定。”第2款规定：“本规定所称区块链信息服务，是指基于区块链技术或者系统，通过互联网站、应用程序等形式，向社会公众提供信息服务。”从私有链的作用来看，其只针对某一组织的内部事务，并不属于“向社会公众提供信息服务”的区块链技术范畴，不是《管理规定》的监管对象。

私有链处于一个中央服务器的控制下，需要邀请才能加入，通常系统的各个节点并非匿名，中央服务器掌握每个节点的所有信息。私有链在企业内部管理中使用，链上的信息大多属于企业经营信息并无大碍，但如果用户包括企业外部人员如金融机构的客户，就可能会产生以下几个方面的问题：

一是隐私权保护问题。用户在上传身份信息时可能会涉及个人隐私，金融机构使用这些信息时必须经过用户的授权或同意。2018年5月25日，欧盟出台《通用数据保护条例》，对个人信息的收集、适用与处理规定了非常严格的保护措施，《通用数据保护条例》将对区块链技术的发展产生重大影响。区块链涉及的加密算法，无论是公钥还是私钥都可能涉及个人隐私或者数据权问题，这些有可能都被《通用数据保护条例》视为个人数据。该条例要求区块链通过设计考虑隐私影响评估和隐私原则（个人数据不能直接而是间接存储在区块链上），提出针对区块链的隐私影响评估框架，以帮助理解这些要求并确保符合《通用数据保护条例》。[①]《中华人民共和国民法典》人格权编第6章专门规定了“隐私权和个人信息保护”，无论是私有链还是公有链、联盟链，涉及相关问题时必须遵守法律规定。

二是知情权问题。区块链系统是在特定计算机网络系统中自动运行的，私有链的共识算法与公有链、联盟链不同，对用户的工作量或者权益不需要工作量证明或权益证明。但是，如果区块链系统的特定算法可能对用户或者相对人的权利义务造成影响，私有链服务提供者就必须对其作出详细说明，并确保用户或者相对人可以准确理解该区块链的运行机制及其可能造成的影响。私有链不同于公有链，由所有用户共同维护、共同协作。因此，私有链的运行对其内部用户和参与者必须公开透明。例如，如果金融机构使用私有链技术为客户提供服务，必须对该项服务内容作详细说明，征得客户同意后才能使用，服务过程也要以信息数据的方式如实存储到系统内，保留历史记录和行为痕迹，任何人或者机构不得篡改。

三是财产权问题。相对于传统管理模式，区块链技术因其电子化与自动化等特点，效率更高、成本更低，去中心化的私有链尤其如此。因此，政府机关、企事业单位如果使用私有链为客户提供服务，不得额外增加客户的经济负担。同时，区块链技术有严密的算法保障其运行的安全性，理应比传统模式更为安全。利用私有链为客户提供服务，必须要保障客户的财产安全，如果出现因为私有链技术问题损害客户利益的，私有链服务提供者必须进行全额赔偿。私有链服务提供者与用户之间往往存在信息不对称以及地位不平等问题，如涉及财产权损害纠纷的案件处理，应该适用举证责任倒置原则。

（四）对联盟链实施穿透式监管

为中共中央政治局讲解区块链技术的陈纯院士认为，联盟链具有高性能、安全隐私、高可用性与高扩展性等四项关键技术优势。[②] 因为这些技术优势，联盟链逐渐成为区块链产业发展的主流。这不仅是产业界的共识，也受到各国政府的欢迎和鼓励。而且与公有链相比，联盟链的社会风险可控，易于被监管。联盟链虽然是多中心化的组织架构，但每个中心节点均为实名，可被准确识别，各方相

① See Simon Schwerin, Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study, 1 The JBBA, 67 (2018).

② 参见陈纯：《联盟区块链关键技术与区块链的监管挑战》，《电力设备管理》2019年第11期。

对独立、信息共享。对联盟链进行规制一方面要对其应用进行监管,另一方面要通过规范化,引导、促进联盟链应用的良性发展。

所有联盟项目必须按照《管理规定》的要求,向国家互联网信息管理部门履行备案手续。同时,由于联盟链的每个中心节点都是独立的,通常有其不同的业务范围,甚至分属于不同的行业。联盟链的每个中心节点的区块链技术既要符合区块链信息管理方面的监管规定,也要根据其应用的领域,接受所属行业监管部门的监管。以平安金融壹账通推出的"天津口岸区块链验证试点项目"为例,该项目基于区块链打造链接各参与方的网络,在保护隐私的前提下实现数据共享,系统可交叉验证加密后的各源头数据,并根据验证后的信息生成通关中的重要单据,降低各方的操作成本和操作风险,构成实现贸易便利化的基础设施。① 这个联盟链的参与者包括海关、银行、运输企业、生产企业及其上下游产业链,除项目本身要接受互联网信息管理部门的监管以外,所涉及的业务还要符合相关行业的法律法规。

联盟链是不同企业主体之间相互协作的技术手段,参与者之间的法律关系应该回归传统法律制度的框架下。从联盟链内部来看,其规范运行和纠纷解决有可能涉及合同法、公司法、侵权责任法等民商事法律。从联盟链外部来看,其规范运行可能涉及行政法、经济法甚至刑法等公法性质的法律法规。需要警惕的是,要防止业务关系有关联的企业利用联盟链技术形成行业壁垒,参与者之间达成垄断协议或者进行经营者集中。一旦出现这种情况,相关部门应该根据反垄断法的规定进行处理。

六、结语

习近平总书记高屋建瓴地指出:"区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。要把区块链作为核心技术自主创新的重要突破口,明确主攻方向,加大投入力度,着力攻克一批关键核心技术,加快推动区块链技术和产业创新发展。"②可以预见,我国区块链技术在相关产业中的应用必将很快进入大发展阶段。从产业的角度看,应当根据不同类型区块链技术的特点,找到适合其应用的场景;从规制的角度看,不同类型区块链技术的规制方法和路径也不尽相同。不仅要对区块链技术的规范发展进行专门立法与专门监管,还要根据其形成的法律关系准确适用传统法律制度、运用既有的监管手段进行规制。区块链是颠覆性的技术,是未来社会的生产关系。如何发挥其技术优势为经济发展与社会治理助力,如何实现科技创新与规范发展相结合,是一个极具时代意义的重大命题。

责任编辑 温世扬

① 参见金融壹账通:《区块链推动建立开放与共享的新金融体系——平安区块链(2019)》,第 14 页。

② 佚名:《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》,《人民日报》2019 年 10 月 26 日。