doi:10.3969/j.issn.1672-626x.2024.04.009

代码信任:一种新型社会信任模式的法治价值

李昆鹏,徐亚文
(武汉大学 法学院,武汉 430072)

摘 要:既有的人格信任无法支撑普泛化的社会信任体制,制度信任也存在救济滞后和交易成本高的缺陷。基于哈希算法、非对称加密技术和共识机制的区块链技术创造了一种新型社会信任模式——代码信任,其具有降低交易成本、预防违约行为和提高可靠性的显著优势。代码信任产生了降低法律运行成本、提高法律治理能力、保证法律公正实施等重要价值,合理使用代码信任可以有效助力法治建设。在代码信任法治价值实现的过程中,建立数字权利凭证是一种可行的进路。此外,区块链技术防篡改性与制度救济之间、代码语言化约性与法律的价值判断和权衡之间的冲突带来了法律风险,需要通过技术与法律的协作加以消除。

关键词:社会信任;代码信任;区块链;法律风险;法治价值
中图分类号:D90 **文献标志码**:A **文章编号**:1672-626X(2024)04-0104-11

一、引言

信任,是根据有限的信息对未来的可靠性所作的潜在性推断,在民商事交互中,又可以具化为对交易活动中可能出现风险的容忍性。信任可区分为个人信任与社会信任,社会信任是指“全体社会成员间存在着的对待公共事务、公共组织、人际交往等社会性活动或机构运作所持有的一整套普遍而近似的态度”[1]。本文使用的“社会信任”一词,意指社会不同群体普遍持有的、对包括交易在内一切社会活动的信任。随着科技发展与社会进步,人与人之间的社会活动呈现范围扩大化、对象一般化、方式多元化的特点,这对社会信任提出了更高的要求。

2008年,中本聪创造性地提出了一种全新的构想,试图建立一种“基于加密而非信任的电子支付系统”,在此基础上区块链系统横空出世[2]。区块链系统基于密码学、共识算法等数学原理,能够使陌生人在无需对交互相对方认识和信任的情形下仍能安心与之交易,构建了一种“无信任的信任”(trustless trust)[3]。区块链系统的诞生带来了一种新的社会信任可能,本文将之称为“代码信任”,人们似乎可以不再依赖他人的品行或制度的庇护,转而诉诸可信的代码系统来保证社会活动的安全。那么,代码信任模式确如想象中完美吗?它存在怎样的优势与风险?它的引入又将给法治建设带来怎样的契机?

目前在法学界,关于区块链与社会信任的研究并不多,这一议题还有较大的研究价值。有学者概括梳理了区块链技术出现后社会信任模式的进一步演变,但未对这种演变展开详细阐释[4];有学者另择角度,依

收稿日期:2024-01-06
基金项目:国家社会科学基金重点项目“弘扬社会主义法治精神研究”(22AZD058)
作者简介:李昆鹏(1999-),男,福建泉州人,武汉大学法学院硕士研究生,研究方向为法学理论;徐亚文(1966-),男,浙江天台人,武汉大学法学院教授,研究方向为西方法哲学、比较法学。

照信任模式是否为中心化结构对其进行分类，并讨论了区块链对社会信任的影响[5]；还有学者重点讨论了区块链技术产生的信任风险[6]。总体而言，当前研究缺乏对代码信任产生机理的详细论述，以及对代码信任如何助力中国法治建设较为明确的构想。结合前文提出的问题与现有研究的不足，下文将逐步说明代码信任的技术基础与优势，并对其法治价值展开阐述。

二、既有社会信任模式及其局限性

关于社会信任模式的分类前人已有很多研究，尼古拉斯·卢曼将社会信任分为人格信任与系统信任，吉登斯则进一步将系统信任细分为对货币、专家和法律等系统的信任，这类分类方法与马克斯·韦伯所称“普遍信任”与“特殊信任”有异曲同工之处[7]。但总体而言，既有的社会信任模式主要可以分为基于特定信任对象的人格信任和基于国家各类救济制度的制度信任，这两种信任模式在不同时期都发挥过至关重要的作用。然而，它们也在根源上存在难以避免的局限性，正因如此，人们对新型社会信任模式的呼声才愈发强烈。

（一）人格信任及其局限性

在原始社会和农业社会中，囿于有限的社会分工和简陋的交通条件，人们进行社会活动的范围相对狭窄，往往仅限于几个部落或村庄中。在这种熟人社会的背景下，为减少甄选社会活动交互对象所需成本，人们往往以信任对象人格的不变本性为基础[8]，通过待交互对象过往行为、口碑等来筛选自己更信任的人，并与之进行更多往来。这种信任模式可以称作人格信任，是最古老、最传统的社会信任机制。

人格信任通过宗法家规、民间习俗和伦理道德体现其约束力，惩戒结果表现为群体压力和关系网的丧失。在熟人社会中，失信人将被宗法家规所惩戒，受戒之人不仅要承受身体或经济上的惩罚，还会在族人面前“抬不起头来”，这将给失信人的生活带来极大的不便利乃至灾难。在宗法家规未涉及之处，亦有公认的习俗与道德来对失信人施压，失信人在内要受良心谴责，在外要受亲朋的冷眼和嘲弄，这种强有力的道德约束使普通人在熟人社会中不会轻易背弃承诺。

然而，“人格信任往往没有弹性，没有长期的互动与经验，不容易转换到另一个人身上”[8]。人格信任的这种特性决定了其并不足以支撑普泛化的社会信任体制。随着科学技术和市场经济的发展，社会越来越需要一个基于制度而非人情的普遍信任模式，在这种背景下，人格信任渐渐丧失了在社会信任体制中的主导地位，成为制度信任的辅助和补充。

（二）制度信任及其局限性

在工业革命之后，大工业生产方式逐步取代了农业生产在社会生产中的主导地位，基于道德约束和个人名誉的人格信任模式难以适应全新的社会环境。在工业社会中，交互双方可能远在千里，人们无从得知相对方的信誉，缺乏判断相对方是否可信的信息基础；此外，由于交互双方已不再共处同一个熟人社会，来自其共同社会环境的道德约束亦不复存在。换言之，名誉与道德的约束功能在此种环境中已完全失效。当人格信任机制逐渐失效，制度信任则以一种不以相对方的身份为基础的信任模式接替它，成为交易活动正常运转的保障。

在制度信任模式中，人们不再完全依赖于交互相对方过往的信誉，而是通过国家法律等一系列制度，在明确双方权利义务的前提下，相信即使对方违约，以国家强制力为保证的制度仍能让自己的权利得到实现。这种信任模式已经脱离了对特定交互相对方的特殊信任，亦非对“制度运作中的人”的信任，而是对整个交易保障机制的普遍信任[9]。正是在制度信任模式的保障下，社会分工进一步深化、交易范围进一步扩大的工业社会中，社会活动的往来才能够稳步、有序进行。

然而，制度信任模式亦非十全十美，制度救济的两大核心弊病使其难以一力承担保障社会活动安全的

重任。其一，制度信任模式中的救济手段具有滞后性。相关法律制度虽以国家强制力为保证，具有一定的事前引导性与规范性，但仍然不能彻底消除违约现象的发生，更多情况下，制度展现其功能的方式是在对方违约之后依当事人申请给予其事后填补损失的权利（诉权）。在救济迟滞的时间内，市场情势与交易发生时可能已产生重大变更，而错失绝佳交易机会、无法进一步扩大商业优势等其他不利益往往只能由当事人承担。其二，制度信任模式中的救济手段将带来繁重的交易成本。如前所述，烦琐的诉讼程序使当事人在寻求救济时需要耗损大量的时间和金钱，行政机关的官僚主义与权力寻租亦为当事人带来了额外的交易成本[5]。正因如此，即使是在工业革命两百余年后的当下，制度信任模式仍未完全取代人格信任模式成为社会活动的不二选择，企业往往会寻找信誉良好的长期合作伙伴以减少可能的纠纷。

步入第四次工业革命之后，区块链技术的诞生使人们看到了一种全新的信任模式——代码信任。在这种信任机制之下，人们不再仰赖特定的信任主体（交互相对方、国家），而是将自动运行的代码作为被信任者，基于对其能够给予有效、合理的正向反馈的信任采取行动。这种全新的信任模式具有独特的优势，随之而产生了新的风险。下文将阐释区块链技术的技术原理与特点，以此为基础展开对代码信任模式的论述。

三、代码信任——基于区块链技术的新型信任模式

本文所称的代码信任，是指以具有防篡改性与可追溯性的区块链技术为核心的信任模式，是对区块链代码的可靠性与有效性足够保障社会活动安全的信任。作为一种去中心化的信任模式，代码信任相较于既有信任模式，具有降低交易成本、预防违约行为和提高可靠性的独特优势，有望为新型社会信任格局提供全新的可能。

（一）代码信任的技术基础

自中本聪提出“区块链”概念以来，区块链经历了三个发展阶段：区块链1.0（货币），此阶段区块链技术的应用仅限于与货币有关的领域；区块链2.0（合约），此时区块链技术的应用延伸至经济、市场、金融领域，如数字产权、智能合约等；区块链3.0（超越），此时区块链技术的应用范围已经超越了货币、金融和市场，成为一项与社会各方面紧密结合的技术[10]。

从本质上来看，区块链是一本由矿工不断创造新区块（账本页），全网各结点共同记录和维护的分布式公开账本[10]，其关键技术包括保证交易可追溯的哈希算法、保护交易数据和用户隐私的非对称加密技术以及实现全网数据一致的共识机制[11]。

1. 哈希算法

哈希函数（Hash function），是一种容易正向求解但无法反向计算的单向函数。它能够将任意长度的数据转化成定长的字段，这一字段被称为原信息的哈希值，哈希值的实质就是原信息的信息摘要。值得注意的是，作为单向函数产物的哈希值无法再还原出原信息，提取信息摘要的过程是不可逆的[12]。为防止不同信息的摘要重复出现，目前广泛使用的哈希算法（MD算法、SHA算法等）均具有很好的抗碰撞性，能够保证输入不同信息时会输出不同的哈希值[13]。因此，一旦原信息在存储或传输过程中丢失或被人为篡改，哈希算法能够快速检测出信息的异动，使用者能够利用这一技术高效验证原信息的真实性和完整性。

比特币区块由区块头和区块体两部分组成，区块头包含这一区块的全部身份信息，区块体则记录这一区块包含的全部交易信息，两者通过哈希算法缠结联系在一起。特别之处在于，区块头还包含了区块链上上一区块头的哈希值，而本区块头的哈希值又被下一区块吸收。这意味着，上一区块的任何异常都会导致其再次生成的哈希值与本区块的记录值不一致，区块链系统会自动拒绝这样的异动。以此类推，各区块通过哈希缠结紧密联系在一起，成为一条“链”，这便是区块链的核心特点。

而区块头与区块体也通过类似的方式进行哈希缠结,区块头中保留区块体内所有交易按照一定方式产生的最终哈希值(默克尔树根,Merkle tree)[14]。类似地,区块体中任一交易发生异动,都将使再次计算出的默克尔树根值与储存值不等,产生牵一发而动全身的效果。如此,无需在区块头中保存每一个交易的详细信息,区块链系统便能自动防止交易信息被他人篡改。

如前所述,哈希算法是区块链技术能够实现防篡改、可追溯的重要保证,它为区块链上储存信息的真实性提供了技术背书,也为区块链带来的代码信任打下了技术基础。

2. 非对称加密技术

"区块链交易之所以不需要第三方信用,根本原因在于其采用密码学原理保障交易安全"[15]。区块链使用了非对称加密技术来确保交易的可信性和个人隐私的安全性。非对称加密技术是指这项加密技术中数据加密和数据解密使用的秘钥不同,在一个秘钥对中,若用秘钥一加密则须用秘钥二解密,反之亦然。

区块链系统采取一种零知识证明(Zero-Knowledge Proof)的加密手段,在系统中,每个用户都会获得一个秘钥对,其中,私钥(private key)由用户个人私藏,不得公开或泄露;公钥(public key)则可以全网广播,作为他人验证自身身份或给自己寄送加密信息的基础。在区块链系统中,通过公钥与私钥的结合就能实现身份验证和信息加密的功能。特别地,用户的私钥、公钥均不与其真实身份挂钩,发起交易时交易内容和金额亦不会被其他结点截取[11]。由此,在不损害用户隐私的前提下,非对称加密技术为交易的可信性提供了技术保证,这使代码信任得以具备一个信任系统的基础功能。

3. 共识机制

在传统中心化数据存储和运行的模式中,全网其他结点都只能向中心结点申请访问账本,对账本的维护和更新都由中心结点独立完成,因此不存在结点之间需要确保数据一致性的问题。但在P2P结构中,如何保证分布式结点维护的是同一个账本则成为不可回避的核心问题。

为解决这一问题,区块链系统开发出了一些共识机制,以保证每一次只有一个结点拥有记账权,其他结点要在该结点开发出的新区块上继续延长这条链。比特币区块链系统使用的共识机制是工作量证明机制(Proof of Work,PoW),该机制要求矿工遍历区块头中的计数器(Nonce),找到一个数使区块头哈希值小于系统规定的难度目标。其中,首个生成合法区块的结点便拥有本次的记账权,其他结点在核验无误后自动认可这一区块,并将之加入区块链。比特币系统会给首个成功的矿工发放比特币奖励,由此激励矿工参与记账[16],这个过程也是比特币系统发币过程。为保证每一个合法区块的生成时间相对稳定,系统会根据当下全网算力定期调整难度目标,以此实现区块链的有序延长。

PoW虽能有效形成全网共识,但每一次"挖矿"的过程都将带来巨大的能源损耗。此外,由于区块生成周期较长,这一机制也带来了比特币系统处理交易速度慢的弊端。为解决上述问题,新兴的区块链系统又实行了若干新型共识机制。但无论是何种证明机制,本质都旨在通过强有力的筛选规则尽可能避免出现区块链分叉,确保全网维护的是同一个账本。共识机制使区块链系统中每一个结点存储和处理的均是相同的数据,这为代码信任中不同主体之间进行信息交互提供了可能。

由此,区块链技术在代码可靠性的背书下,为交易双方引入了一个既不逐利也不偏心的"上帝":他保护双方的隐私安全,不需要抽取佣金就愿意为交易双方牵线搭桥,保证交易安全进行[15]。

(二)代码信任的优势

相较于传统的人格信任与制度信任,以区块链技术为基础的代码信任模式在以交易活动为代表的社会活动中具有三个显著优势。

1. 降低交易成本

事实上,寻求代码信任并非保证互联网安全交易的唯一方式,当前电子商务行业中最成熟的模式是"商

家对顾客”(Business to Customer,B2C)模式,即商家和顾客在第三方平台上进行交易,第三方平台作为权威中介监管交易的安全进行并收取中介费。第三方平台的规模与声誉直接决定交易双方是否信任平台。不难发现,寻求权威中介监管交易的B2C模式本质上仍是传统人格信任模式的变体,只是此时交易发起方无需对相对方有信任,而是转而信任第三方平台,但仍然排除不了对信任关系中信任主体的依赖。这些第三方平台不会出于慈善目的监管交易,自身会从每一笔交易中抽取佣金或定期向商家收取“入驻费”,这些额外交易成本最终都将由交易双方承担。更有甚者,不断扩张的第三方平台进一步强化了中心化信任带来的垄断问题,为降低交易成本而生的平台反而成为了交易双方的最大壁垒[17]。制度信任也无法规避繁重交易成本的问题:为使自身权利能够更好获得保护,交易双方需要聘请律师拟定合法、完善的合同;一旦出现交易争端,举证费用、律师费等高额诉讼成本也难以避免。

区块链技术能够使陌生人之间的信任成为可能,而信任问题的解决将从根本上降低交易成本。区块链系统的代码并不逐利,也没有偏好,用户只需注册一个账户便可通过区块链系统完成交易,无需向系统支付额外费用;交易过程所有结点的账本同步更新,免除了事后对账带来的交易费用与延迟。因此,代码信任模式下,交易双方可以以最低的交易成本实现安全交易,这将会改变交易活动中信任机制的新格局。

区块链技术也能与制度信任相结合,在现有机制下减轻交易当事人的负担。诉讼成本的一大部分来自诉讼证据,当事人取证、存证、举证的过程需要耗时耗力,最终证据却不一定能获得法院的认可。2012年前后,电子证据作为一种新的法定证据类型进入了法律条文,这为诉讼双方降低证明成本提供了一条可能的新路径。然而,法院对电子证据的采信率并不高,甚至在近69%的案件中,法院明确不认可电子证据的证明力[18]。究其根本,是因为电子证据容易被技术人员后台篡改,保管电子证据的硬件一旦出现故障也将导致其真实性大打折扣,法院自然对电子证据的认可度较低。有学者主张电子证据亦有较强的稳定性与真实性,只需进一步考察该证据的附属信息与痕迹信息即可判断电子证据是否可靠[19]。但在现实生活中,当事人提出证据时很少提供这些补充信息,即使当事人向法院提供了这些信息,一般法官也不具备鉴别其真伪的能力,电子证据采信率低的现状仍然难以改变。

区块链的出现有助于提高电子证据和其他能够电子存证的证据的可信度。如前所述,区块链技术具有天然的防篡改性,尤其当一个区块位于区块链较前端的位置时,几乎无法在技术上篡改该区块的数据,因此,它能够为上链后的证据不再受篡改提供背书。2019年,杭州互联网法院在一起著作权纠纷中认定经区块链存证的证据有自证其真、防篡改的特性,开创了中国法院认可区块链存证的先河①。在区块链技术的帮助之下,诉讼人无需亲身前往公证处、缴纳公证费便可得到法院认可的可信证据,这能极大降低其诉讼成本,提高其未来参与交易的积极性。

2. 预防违约行为

无论是人格信任所仰赖的道德规范,还是制度信任所依据的法律法规,都没有在交易发生前绝对防止交易一方违约的功能。它们虽均以制裁为保障,具有一定的恫吓与约束效果,但最终交易一方是否违约仍取决于他们内心对规范是否存有足够的敬畏。换言之,两种传统的信任机制最重要的功能仍在于提供事后救济。事后救济手段虽也能保护当事人的利益,但其效果常常不尽如人意,从强制执行程序中常出现的执行不能、“老赖”可见一斑。

代码信任对这一问题作出了有效的回应。基于区块链系统的可信运行环境与Nick Szabo对智能合约的构想,Vitalik Buterin创建了支持智能合约的区块链2.0项目——以太坊[20]。智能合约是一个自执行系统,用户可以利用图灵完备的编程语言将合同触发条件写入代码,智能合约通过预言机与现实世界交互输入事件,并在触发预定条件时自动执行合同[21]。执行智能合约实际上是用户从外部账户往合约账户发起交易的过程,在执行时,用户支出的以太币金额不得高于其拥有的余额,否则交易就会失败。如此,以太坊的自动

执行机制杜绝了交易一方失信的可能性，从根本上实现了预防违约行为发生的功能。

3. 提高可靠性

既有的两种社会信任模式虽然逻辑有差异，但本质却都属于人对人的治理。在人格信任模式中，信任对象的品性直接决定了这段信任关系是否可靠稳定，然而，基于个人品性的人格信任过于依赖个人的道德水平，从根源上充满着不确定性。基于抽象系统的制度信任能够较好地解决这一问题，但从更现实的视角来看，抽象的制度仍需经过具体的自然人来运作，一旦位于制度关键结点的个体出现贪腐、渎职、滥权等行为，很容易导致系统暂时性失灵。完善的制度会在其纠偏机制的作用下逐渐回到正轨，但短暂失灵对当事人的影响也难以快速消除。因此，难以彻底摒除人类劣根性的制度信任模式亦无法给予交易双方完善、全面的保护。

代码信任的实质是将社会信任寄托于技术，这种摒除了被信任者主观倾向与不对称信息干扰的信任模式可以有效规避失信风险[22]。在代码信任模式中，一旦区块链代码成型，其运作不再依赖于任何个人，即使是软件开发者在征得全网共识之前也无法变更或妨碍区块链的运作。但需要注意的是，这并不意味着区块链上的交易无需任何人参与。在比特币系统中，为使交易尽早入链，交易发起者往往会给“矿工”留下一定的交易费。由于比特币系统未能明确规定交易费的标准，有研究人员担心在比特币发行数量减少后，交易费将会陷入无序攀比的乱象，甚至演变为赤裸裸的对矿工的贿赂[11]。所幸这一问题在以太坊中已得到较好的解决，以太坊采用的Gas机制使智能合约的交易费与其复杂程度呈线性正相关关系，智能合约的复杂度上升，交易费也随之上涨，由此避免了交易费的无序竞争。在交易费受到有效规制后，可以说代码信任彻底摆脱了对人的依赖，交易双方需要信任的只有代码本身。代码并不十全十美，但它没有人类的逐利与怠惰，在这个意义上，相较于人格信任与制度信任，代码信任是更为可靠的信任机制。

此外，相较于现有的中心化信任结构，代码信任的数据存储是高冗余分布的，每个结点都存有完整的数据副本。这意味着没有任何机构或个人能够单独篡改过往数据，任何一个或几个结点损坏也不会破坏系统的信任结构，这进一步提高了代码信任的可靠性。

四、代码信任对法治价值的增益

“（区块链系统）合法实践范围本质上是一个治理问题，而非计算机科学问题”[3]。代码信任能否成功融入法治建设的进程，从根源上仍取决于人们以怎样的方式使用代码信任。前文中论述的区块链多为非许可的公有链，加入这种区块链的结点无需额外获得系统的授权和认可，只要安装相应系统便能直接加入区块链主网。但允许结点随意出入、采取行动需获得全网结点共识的公有链不利于现行法律的介入与管理。一方面，在公有链上任何版本的迭代或更新都需要全网结点共识，效率低下且难以推行，不利于法律强制性介入；另一方面，允许匿名制结点随意出入区块链，与灰黑产业相关的非法合同便难以禁止，新的区块链恐又会像比特币系统一样成为滋养犯罪的温床[23]。

为了更好体现代码信任的法治价值，可以选择用联盟链来替代公有链。联盟链是指仅有经过授权的联盟结点才能加入的区块链，在联盟链中各结点的读写权限、记账权限均由联盟规则来制定。由于采取许可加入和协议验证的方式，联盟链相较于公有链能实现更快的交易处理速度、更低的交易成本以及更有效的系统控制[24]。可以依据具体需求建设不同的联盟链，如政务区块链、司法区块链、医疗区块链等，在这些联盟链中充分发挥代码信任的优势，助力法治建设。

（一）实现数据高效流转，降低法律运行成本

当前，在公民办理政务、不同部门之间交接手续等情境存在法律运行成本较高的问题，主要是各主体之

间数据共享存在障碍所致。为此，在政府机关内部的数据共享问题上，我国按照“一数一源、一源多用”的原则，构建了数据共享中心[25]。2019年，我国上线运行了国家政务服务平台，并以此为枢纽，结合各地区地方性数据共享平台，打造了全国一体化在线政务服务平台；2022年，《国务院关于加强数字政府建设的指导意见》进一步提出了“深化数据高效共享”的要求。然而，当前运行的这一平台对数据的高效流转仍有两个主要障碍。其一，作为一个中心化平台，它的运行与维护都依赖于中心结点的正常运转，一旦中心结点出现故障，平台上的数据安全和可信度将会极大降低。其二，平台上的数据流转仍是一个数据供给方从本地数据库取出、上传，平台审核并保存，数据需求方下载、保存的过程，不仅过程较为烦琐，增加了数据丢失和疏漏的风险，也导致了不同系统间信息共享实时性、标准一致性低和相互信任难的问题。因此，这种数据来源分散、逻辑结构集中的平台上数据可信性仍是由平台自身的稳定性和数据供给方的认真负责来保障的，没有更为稳定和可靠的背书，难以真正实现数据高效共享。

代码信任模式或可助力解决这一问题，即由中央政府牵头打造一条数据共享联盟链，地方相关部门作为核心结点加入。根据具体需要，可以此为基础使用侧链技术根据需要建立分支链，保证不同部门之间个性化的可信数据共享需求。在这一机制中，分布式的数据储存和链式缠结结构能保证数据的可信性，相较于中心化结构，P2P的数据传输结构和全网共识的数据集可以保证数据的高效流转。我国正在打造的司法区块链可以视为这一模式的成功实践。2022年5月25日，最高人民法院发布《最高人民法院关于加强区块链司法应用的意见》（法发〔2022〕16号），要求到2025年“建成人民法院与社会各行各业互通共享的区块链联盟”。当前，已有部分司法区块链成功落地，例如苏州市相城区人民法院已与当地不动产管理中心实现了区块链联动，当事人仅凭裁判文书中所附区块链二维码便可在不动产中心完成不动产变更登记，极大简化了办理程序[26]。

未来，司法区块链可以进一步自下而上整合，先在地区内实现不同法院区块链之间的跨链联动，而后逐层向上直至实现“全国一条链”的构想。由此可见，“区块链+司法”的应用方式也可全面扩展为“区块链+”的模式，实现公权力机关内部、公权力机关与市场主体等多元主体间的数据互通，最大化降低制度运行成本，以期获得社会资源分配的帕累托最优。

（二）维护数据公开透明，提高法律治理能力

在法律治理过程中，被监管主体的过程数据不透明一直是监管难的重要症结。在医疗领域，电子病历的数据控制权牢牢掌握在医院手中，在当事人与医院发生纠纷时，常因医院是否擅自篡改病历数据而存在争议；在慈善捐赠领域，善款来源去向不明、慈善机构信息披露不充分等现象时有发生，这些问题不仅挫败了公众对慈善机构的信心，也让法律难以对慈善机构进行有效监管。除了医疗和慈善领域，在假冒伪劣产品、公司审计等场景中，核心数据披露的缺位也都给法律监管带来极大的障碍。

在代码信任模式中，各方共享数据，且链上数据具有防篡改、可信度高的特征，可以此为基础提高法律的治理效能，在各领域建立起相应的联盟链不失为可行的解决之道。在联盟链中，参照Corda平台，为监管部门设立具有可读权限（必要时可具有可写权限）的监管结点，在监管结点的监督下让链上的数据披露和流转有序进行[16]。如在医疗领域，可以利用区块链为医院、患者、第三方机构设置相应的读写权限，在保证患者病历安全性的同时使其便利地在信息需求方中流动[27]，医疗机构的任何修改记录都会被留存，也消除了法律监管的障碍。又如在慈善捐赠领域，代码信任的革新可以更进一步，直接利用可信系统和智能合约替代慈善机构，构建捐赠人与受助人的直接联结关系，保证善款来源和去向的透明性[28]。在慈善链上，公权机关可以直接利用访问权限监管每一笔善款的去向，防止第三人非法使用和占有。以此类推，在防伪溯源、公司审计等领域，都可通过构建联盟链的方式寻求因应之道，实现待监管主体充分的数据披露。尤其是在应急管理中，这种基于数据透明和实时共享的代码信任模式可以在最短时间内高效、精准地匹配供需关系，调配所

需资源,在应急事件发生时有效提高法律治理能力。由此,在代码信任模式中,虚假数据和隐匿侵占无所遁形,法律的治理效能也得以显著提升。

(三)构建可溯执法模式,保证法律公正实施

在人类社会民主政治的演进过程中,对权力的监督与制约是永恒的议题。作为国家权力的代表,执法者的行政权力应当受到严格的监督与约束,只有执法者都在"制度的笼子"中用权,法律给予公民"人人平等"的承诺才能够实现。当前,我国实行的权力监督机制尚存在异体监督主客体目标不一、同体监督人情关系难摒弃的问题[29],执法过程缺乏统一的可信记录、执法结果与执法行为之间缺乏数据关联等现象也给我国的执法监督带来了障碍。

为应对这些问题,需要尽可能留存可信的执法数据,以此为基础建立执法结果与执法行为之间的可视化关联,在执法结果出现明显偏差时进一步依据可溯源的执法数据启动问责机制。一言以蔽之,这一过程需要权力监督机制从纯粹的"人管人"逐渐向"技术管人"过渡。代码信任能够促成这一目标的实现,其可以利用区块链技术全面记录每一执法行为的过程。在源头处记录审批者与具体执行者,在过程处记录执行方式及罚款的来源与去向,在结果处要求被执行者在确定前述数据无误后方点击确认,由此构建"源头可溯、过程可查、责任可追"的全流程执法监督格局。而法律规定的权力监督主体则作为监管结点在这条链上全方面监管每一个执法行为,保证对执法行为监督的实时性和可视性,降低监督过程的滞后性。如遇到法律规范清晰,行政机关自由裁量权小的执法行为,可以预先设置智能合约,当事人只需点击智能合约便可自动完成执法过程,进一步减少对执法人员的依赖,压缩权力寻租的空间。

五、代码信任与法治价值的实现

如前所述,代码信任能够在多个维度为法治建设带来增益,然而,其法治价值的具体实现既是机遇,也会带来风险。下文将从代码信任法治价值的具体实现进路和法律风险的消除两方面进一步展开论述。

(一)建立数字权利凭证,创新权利保护范式

作为一种可信分布式账本,区块链上的数据都具有全网共享、可信度高的特质,这使其有助于建立一种全新的数字权利凭证。如在证券交易领域,可利用区块链的可信储存建立证券资产凭证,使其替代证券公司成为新型可信交易结构。

基于代码信任的权利保护范式还可扩展至更多的场景,以版权保护为例,理论上,版权经登记后可以受到更好的保护,然而在实践中,一方面,复杂的版权登记制度降低了作者版权确权的积极性,给其权利保护带来了障碍;另一方面,数字化作品的无限可复制性导致侵权作品在互联网上大行其道,且这些侵权作品的来源难以追溯,作者对这种情况常常只能听之任之,无法有效维权。

然而,运用代码信任模式,可以提高版权保护效力。即由国家知识产权局协同有关部门建立联盟链,或建立以版权管理链为主链,版权确权链和运用链为侧链的多源异构架构进行协同管理[30]。具体而言,可将该版权确权链作为版权的合法登记手段,以区块链的时间戳(可信时间证明)与防篡改性为版权权属背书;利用版权运用链上自动运行的智能合约,替代当前的版权集中管理组织,自动实现版权的许可、转让;前述所有信息都存在具有防篡改性的区块链中,可成为出现争议时的可信证据。由此,代码信任相较于传统分离式管理能够实现对作品"确权、用权、维权"的全生命周期集中化管理,开创全新的版权管理模式。

在国外已有Binded、Monegraph等平台正在提供数字版权相关服务[31],在国内百度图腾等版权区块链也在运作[32],但这些平台尚未与相关部门有效联动,公信力仍有不足,只能作为未来进一步利用代码信任保护版权的雏形。此外,还可以利用区块链防伪溯源的功能对纸质作品进行全流程管理,有效防止盗版与窜货

现象。可见，代码信任能够助力建立新型权利凭证，开创全新的权利保护范式。

（二）建立技术-法律协作，消除代码信任风险

当然，任何新技术的运用都可能存在与既有法律秩序的冲突，在发挥代码信任优势的同时，也需要警惕代码信任与当前法律存在不兼容之处[33]。

首先，区块链技术防篡改与制度救济之间存在较明显的冲突。以法律为代表的国家制度对于交易中的受害方往往有较为完备的事后救济制度，这是国家公信力对交易参与方的承诺。例如，依据《民法典》第一百四十七至一百五十一条，当交易一方受胁迫、欺诈或出现重大误解、显失公平等情形时，该当事人享有撤销权，在满足一定条件时有权行使形成诉权，使该合同不实施。

在区块链系统中，交易一旦上链就很难更改，在公有链中，较为可行的方式仅有发起一笔新交易以返还原交易支付的金额。但这样的处置方式至少存在两个弊端：其一，法院无法直接介入公有链的交易发起和认证机制，只能“监督”当事人重新发起一笔原交易的逆交易，这给法院带来了更大的执行负担；其二，公有链多为匿名链，交易当事人难以得知对方究竟是否为适格的交易主体，遑论在该交易受追认前行使撤销权，在这种情形下，一旦未来该交易未受追认，该善意当事人的权利将会受到侵害。

为降低这一风险，可以要求交易双方在智能合约编写伊始便有法律人员参与，实现法律对智能合约全过程的指导和监管。具体而言，可由律师拟定纸质合同作为正本存档，而后委托技术公司依据纸质合同复刻出智能合约，打造李嘉图式合约（Ricardian Contract）[34]。若未来出现合同纠纷，法院以纸质合同作为合同原本进行解释和裁判，并另行采取线下执行方式回复当事人所受损失。

其次，代码语言化约性在一定程度上排斥了法律的价值判断与权衡。自古而今，鲜有学者认为法律是一种清晰可知、确定不移的文本。无论是哈特所说的“开放性结构”还是德沃金所强调的“法律原则”，都是在强调如下事实：“为了使用包含一般化分类语汇的传播形式来传达实施情况，（法律语言）边界地带的不确定性是我们必须要付出的代价”[35]。如果法律在任何时候有唯一的“正解”，法学学者也不必为法律应当如何解释而产生争论。例如，对于民法典规定的“显失公平”“重大误解”等模糊性概念往往需要法官在具体情形中进行价值判断方能准确适用，而代码语言却无法实现这项功能。代码语言以严谨但机械的数学结构为基础，本质上只是若干if-then语句的叠加和嵌套，只能在确定无疑的情形下执行。智能合约本质就是一段存储在区块链上的代码，因此，智能合约也面临同样的问题，它具有明显的“刚性”，不能灵活变通[36]。而难以作出价值判断的智能合约，在需要对合同条款作解释的情形下可能会克减一方当事人的部分权利或加重其义务。尤其是在“代码即法律”的模式中，作为代码的智能合约绝对产生约束力，不容当事人更改[24]，这使得智能合约无价值判断的问题变得越发严峻。

尽管代码难以体现价值判断与权衡，至少较长一段时间内，智能合约还不能取代需要包含灵活条款的传统合同，但可以利用多重签名技术（Multiple Signatures，MS）在智能合约执行过程中引入第三方裁判者，即由交易双方当事人各持有一把秘钥，裁判者（如法院）持有第三把秘钥，要求该智能合约至少须有两把秘钥签名才会执行。在这一模式中，只要双方当事人出现异议，裁判者就将终局决定智能合约是否执行，如此，便能成功将复杂的价值判断问题复归于权威裁判者处理。

六、结语

基于对人格信任、制度信任两种既有信任模式的综合考察，本文分析了既有信任模式的局限性，并以此为基点对基于区块链系统的新型信任模式——代码信任模式进行研究。代码信任模式具有降低交易成本、预防违约行为和提高可靠性的显著优势，能够作为既有社会信任模式的重要补充，助力建设更良好的社会

信任格局。

代码信任在法律运行的各个维度上具备重要价值，合理利用代码信任对外可以提高法律治理能力、对内可以强化法律监督机制，此外，代码信任还能起到降低制度运行成本的效果。开创新型权利保护范式可以视为代码信任助力法治建设的成功范例。

在发挥代码信任优势的同时，需要警惕区块链技术防篡改性与制度救济之间的冲突，以及极具化约性的代码语言难以实现价值评判等风险。此外，如前所述，为了维护公有链共识而产生的能耗也是难以忽视的社会问题。盲目将公有区块链作为新型信任模式的基础存在较高风险，兼具区块链与传统治理模式优势的联盟链或许是替代公有链成为新型信任模式基础的更好选择。因为联盟链的共识取决于核心结点之间的协议，对共识机制的要求较低，不需要采用PoW这种高能耗共识机制；此外，核心结点群拥有对联盟链的绝对控制权，可以利用传统治理模式的优势有效降低区块链技术对现行监管体制的冲击。

总之，依托于技术发展而形成的代码信任模式将进一步推动普遍信任替代特殊信任、系统信任替代人格信任的社会发展进程，在各个维度上为我国法治建设作出新的贡献。

注　释：

① 参见杭州华泰一媒文化传媒有限公司诉北京阳光飞华科技发展有限公司侵害作品信息网络传播权纠纷一案，(2018)浙0192民初9655号。

参考文献：

[1] 白春阳.社会信任的基本形式解析[J].河南社会科学，2006(1)：4-6.

[2] SATOSHI NAKAMOTO. Bitcoin：A Peer-to-Peer Electronic Cash System[EB/OL].[2023-08-25].https://bitcoin.org/bitcoin.pdf.

[3] KEVIN WERBACH. Trust，but Verify：Why the Blockchain Needs the Law[J].Berkeley Technology Law Journal，2018，33(2)：487-550.

[4] 张清，郭胜男.人际信任、法律信任与数字信任：社会信任的谱系及其演进[J].哈尔滨工业大学学报(社会科学版)，2021(6)：51-57.

[5] 郑观，范克韬.区块链时代的信任结构及其法律规制[J].浙江学刊，2019(5)：115-123.

[6] 徐祥运，高海鑫.区块链技术对社会信任模式的影响及所致信任风险的防范[J].学术交流，2023(1)：122-135.

[7] 李伟民，梁玉成.特殊信任与普遍信任：中国人信任的结构与特征[J].社会学研究，2002(3)：11-22.

[8] 伍德志.论法律信任建构的反向逻辑：不信任的制度化及其功能[J].暨南学报(哲学社会科学版)，2023(3)：54-71.

[9] 房书君，崔静，王明文.法律信任及其在当代中国的建构[J].东北师大学报(哲学社会科学版)，2016(1)：234-237.

[10] [美] 梅兰妮·斯万.区块链：新经济蓝图及导读[M].韩峰，主编.北京：新星出版社，2018.

[11] 凌力.解构区块链[M].北京：清华大学出版社，2019.

[12] 王思远，张华.区块链概论[M].北京：北京大学出版社，2021.

[13] 袁勇，王飞跃.区块链技术发展现状与展望[J].自动化学报，2016(4)：481-494.

[14] H. LIU，X. LUO，H. LIU，X. XIA. Merkle Tree：A Fundamental Component of Blockchains[C] //.2021 International Conference on Electronic Information Engineering and Computer Science(EIECS). Changchun，China：IEEE，2021.

[15] 赵磊.区块链技术的算法规制[J].现代法学，2020(2)：108-120.

[16] [美] 凯文·韦巴赫.区块链与信任新架构[M].北京：机械工业出版社，2020.

[17] 杨继.区块链、互联网信任与制度设计[J].上海经济研究，2021(6)：27-38.

[18] 刘品新.印证与概率：电子证据的客观化采信[J].环球法律评论，2017(4)：109-127.

[19] 刘品新.电子证据的基础理论[J].国家检察官学院学报，2017(1)：151-159.

[20] JANI S. Smart Contracts：Building Blocks for Digital Transformation[D].Indira Gandhi National Open University，2020.

[21] O'SHIELDS R. Smart Contracts: Legal Agreements for the Blockchain[J].North Carolina Banking Institute, 2017, 21: 177-194.
[22] 徐延辉,吴世倩.区块链技术与数字信任建构机制研究——以百度超级链为例[J].南京社会科学,2022(9):55-64.
[23] ENGLE E. Is Bitcoin Rat Poison: Cryptocurrency, Crime, and Counterfeiting(CCC)[J].Journal of High Technology Law, 2015, 16: 340-393.
[24] 王延川,陈姿含,伊然.区块链治理:原理与场景[M].上海:上海人民出版社,2021.
[25] 邢会强.政务数据共享与个人信息保护[J].行政法学研究,2023(2):68-81.
[26] 郑卫平,居丹丹.当司法"遇见"区块链[N].人民法院报,2023-08-01(8).
[27] 史雅妮,陈嘉曼,李晨瑜,等.破解电子病历信息共享困境:区块链的转型干预作用[J].图书情报知识,2022(6):20-34.
[28] 崔军,颜梦洁.区块链赋能慈善捐赠协同治理的框架与应用[J].学术探索,2022(10):117-124.
[29] 王公,张博颖.区块链赋能公权力监督:问题成因、逻辑耦合与挑战应对[J].领导科学,2023(6):115-118.
[30] 胡剑,戚湧.多源异构视域下基于区块链的知识产权协同管理模式研究[J].科技与法律(中英文),2022(6):73-82.
[31] REBECCA-GEORGIA DUNCA. Blockchain & Copyright - A Revolution in Creativity[J].Romanian Journal of Intellectual Property Law, 2022(3): 126-145.
[32] 刘宗媛,刘曦子.区块链在数字版权领域的应用[J].网络空间安全,2019(12):36-45.
[33] WEINSTEIN S N. Blockchain Neutrality[J].Georgia Law Review, 2020, 55: 499-591.
[34] I. GRIGG. The Ricardian Contract[C] //First IEEE International Workshop on Electronic Contracting, San Diego, USA: IEEE, 2004.
[35] [英]哈特.法律的概念(第3版)[M].许家馨,李冠宜,译.北京:法律出版社,2018:7.
[36] 谭佐财.智能合约的法律属性与民事法律关系论[J].科技与法律,2020(6):65-75.

(责任编辑:何 飞)