重庆大学学报(社会科学版) 2019年第25卷第3期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 25 No. 3 2019

Doi:10.11835/j.issn.1008-5831.fx.2018.11.004

欢迎按以下格式引用:倪蕴帷. 区块链技术下智能合约的民法分析、应用与启示[J].重庆大学学报(社会科学版),2019(3):170-181.

Citation Format: NI Yunwei. Civil law analysis, application and enlightenment of smart contract under blockchain technology[J]. Journal of Chongqing University(Social Science Edition),2019(3):170-181.

区块链技术下智能合约的民法分析、应用与启示

倪蕴帷

(南京大学 法学院,南京 210093)

摘要:区块链被称为第四次工业革命的发动机,是具有普适性的底层技术框架,它不仅与民法息息相关,更有可能深刻改变传统私法领域的既定规则。区块链使用了独特的方式对现实世界交易流程进行模拟,因而能被民法原理所解读,并加以拓展和运用。在其之上建立的智能合约技术,被认为可能引发金融、法律活动的深度蜕变,通过将合同内容进行数字化编码并部署于区块链上,使合同的履行过程能够以一种去中心化、去信任、高度自治的方式进行。然而智能合约并未超越现有的法学概念,它的实质是运用技术手段在合同或要约之上添加辅助履行的担保功能,使合同指向的财产利益能得到确定移转。从现有发展来看,区块链及智能合约技术尚处于初级阶段,绝大多数应用都集中在定型化的虚拟场景之中,离全面普及仍有一定距离。智能合约还有多重法律及技术瓶颈,在诸如编码漏洞、语言转化、现实交互、跨国监管等问题上存在一系列风险与挑战。

关键词:区块链;智能合约;比特币;以太坊;合同法

中图分类号:D923 **文献标志码**:A **文章编号**:1008-5831(2019)03-0170-12

引言

自中本聪论文《比特币:一种点对点的电子现金系统》问世以来[1],比特币从萌芽、发展至成熟已近10年。截至2017年8月,其全球市值突破700亿美元,每一单位比特币价格达到每盎司黄金的3倍以上。德国政府于2013年承认比特币的合法货币地位,拥有者可以使用比特币缴纳税金。全球各大企业陆续接受数字货币支付,在取消比特币消费税之后,日本约26万家商店正式开启比特币支付通道。比特币诞生至今饱受争议,支持者强调其去中心化、抗通胀特征,高效便捷的跨境支付结算以及优质的投资潜力,反对者则将它比作击鼓传花、庞氏骗局。法学界的研究成果主要集中虚拟货币的法律属性、税收政策,以及各国金融监管的比较评述等领域,对于比特币的底层原

修回日期:2018-11-07

作者简介:倪蕴帷(1991—),男,江苏南京人,南京大学法学院博士研究生,主要从事民商法研究,Email:waaaaaagh@qq.com。

理——区块链技术(blockchain),一种建立于共识机制上的分布或账本所具有的私法构造与应用前景,关注者寥寥。

区块链技术被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新,将在全球范围引起一场新的技术革新和产业变革①。区块链被国务院列入《"十三五"国家信息化规划》,要求加强基础研发和前沿布局,从国家科技战略层面肯定了它的技术与社会价值,美国、英国、日本政府也相继出台区块链研究报告。中国人民银行挂牌成立数字货币研究所,积极发掘与探索区块链技术潜力。这一技术也获得了金融巨头的青睐,成为金融科技领域(fintech)最受关注的话题之一。纳斯达克于2015年推出了基于区块链的证券交易平台Linq,花旗银行、摩根大通、高盛集团都相继开展区块链实验项目,推动技术落地。区块链将分布式的思维引入经济与法律范畴,创造了一种基于技术的社会信任体系,以实现对中心化机制的颠覆。区块链是具有普适性的底层技术框架,它虽根植于密码学和计算机原理,却是对现实世界交易流程的模拟和重构。因此不仅与民法息息相关,更有可能深刻改变传统私法领域的既定规则。

而在区块链的前沿应用中,最为瞩目的——正如欧洲议会在其报告中所指出的那样[2],当属智能合约(smartcontract)。智能合约直译应为"智能合同",是指基于区块链的、可直接控制数字资产交易的计算机程序[3]。智能合约最初以自动贩卖机为构想,将合同文本通过程序逻辑编译及运行,以实现与外部信息的交互。在区块链语境下,智能合约的代码被部署在分布式、可复制的账本上,可以接收、处理、储存和发送,使合同条款的自动执行成为可能。智能合约技术目前已在证券、抵押、保险、土地所有权登记等领域产生了一些初级应用,未来将有广阔的前景并可能引发经济、法律活动的深度蜕变。激进的学者认为智能合约会导致传统合同法的终结,大幅改变甚至取代律师和法院的社会功能[4]。那么智能合约究竟是什么?它与传统合同有何种区别与联系?本文将运用民法学原理,对区块链技术下智能合约的法律构架进行剖析,以期为深入探讨与研究提供些许借鉴。

一、区块链技术原理的民法分析

比特币是区块链第一个和最为知名的应用,使区块链技术通常与虚拟货币相绑定,实际上它的应用场景远不止于此。区块链作为一种通用技术原理,能被用于构架可编程的货币系统、支付系统、供应链管理、信息记录等[5],并延伸至整个私法范畴及金融体系。区块链技术的本质,是一种由多个独立节点分散记录的分布式账簿(distributed ledger),是将全部交易记录按时间序列组合成区块结构,并以密码学方式保证的不可篡改和不可伪造的去中心化数据库[6]。由于它是一种关于认证和检验的技术,因此可以更高效地确认及转让所有权凭证。由于它是可编程的,使"智能合约"的自动执行成为可能。由于它是去中心化的,所以能够在无须信任中心机构的情形下实施上述功能。由于它是无国界和无中介的,因而可提供一个高效便捷、极低费用的价值传输途径[7]。区块链技术通过将系统部署以来的全部交易过程封包记录于区块之中,同时为每一笔交易盖上时间戳,以保证交易记录的不可篡改和账簿的唯一性,故又被称作分布式账簿技术(distributed ledger technologies,DLTs)。

所谓分布式账簿,即是说区块链网络中的每一个节点都拥有一份记录交易信息的账簿,同时这些账簿通过工作量证明(proofofwork,PoW)或其他方式保持完整性与同一性。对于传统民法预设的交易场景而言,一笔交易通常由私主体之间作出意思表示,当双方达成合意时合同成立。例如,A

①参见:工信部《中国区块链接技术和应用发展白皮书》(2016年)。

与 B 订立房屋买卖合同,由 A 向 B 作出购房要约,B 向 A 作出购房承诺,意思表示只在交易双方之间传递。在区块链构架中,每一笔交易信息不是向交易对方作出,也不是向某个中央数据系统作出,而是向整个区块链网络节点进行广播。以比特币的区块链系统为例,A 与 B 达成交易 5 个比特币(bitcoin,BTC)的合意,A 不是将交易信息直接发送给 B,而是将此条交易信息发送给比特币网络中的每一个人。区块链通过非对称加密后的公钥、私钥来标识身份,A 以自己的私钥与 B 的公钥对该交易信息签名,全网络节点都接收了这项交易信息,但只有 B 可以通过自己的私钥进行解密。因此对于区块链中的交易,不仅需要交易双方达成意思表示合意,还需要将合意的内容向全网络公示,以保证各个节点的账簿中都记录下了此项交易。

区块链网络中的每个节点都可以通过特定的哈希算法和 Merkle tree 数据结构,将一段时间内接收到的交易数据和代码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[6]。对比特币而言,每 10 分钟内发生的全部有效交易都会被统一记录在新增区块中,每个区块包含一个时间戳、一个随机数、一个对上一个区块的引用(即哈希,hash)和上一区块生成以来发生的所有交易列表。区块按时间顺序相互链接不断更新,以保持比特币账簿的最新状态,区块链由此得名。A 向 B 转让 5 个比特币的交易信息向全网络节点广播,节点通过验证哈希值认可交易的有效性,随后存有该交易信息的区块被盖上时间戳添加至区块链中,成为一条任何人可以查看,永久而透明的交易记录。比特币账簿中记录了从 2009 年创世区块建立以来的全部交易记录,A 与 B 拥有的比特币数量,可以通过这些交易记录追本溯源计算得出。所以区块链网络中人手一本的分布式账簿相当于房屋登记簿,代表了区块链资产的所有权凭证,而这种所有权是通过全部交易记录的相互叠加来确定的(见图 1)。

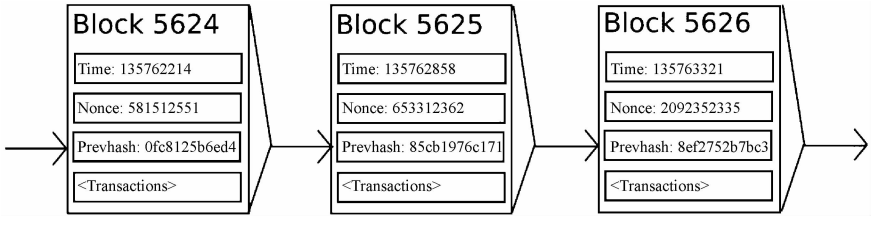

图 1 区块链数据结构

不同网络节点之间如何保持账簿的同一性? A 拥有的 5 个比特币在同一区块下分别向 B、C 作出两笔交易,并向不同网络节点进行广播。由于比特币系统内节点众多且采用点对点扁平式拓扑结构相互连通和交互,同一交易信息无法迅速广播至全网络,不同节点账簿中可能同时存在 A 与 B、A 与 C 两笔交易,如何避免这种“一房二卖”现象即是密码学领域经典的双重支付与拜占庭将军难题。双重支付又被称作“双花”,即利用数字资产的虚拟特性两次或多次使用同一资产完成交易[8]。拜占庭将军难题则是指在缺少可信任的中央节点的情形下,如何允许一定数量的失效而不影响系统整体的可靠性[9]。区块链资产不具备物理实体,不能通过动产的占有表征所有权,也没有第三方中心机构(如房产局)记账,因而无法使用传统的不动产所有权登记进行证明。针对此问题,比特币系统创造性地设计了一种基于工作量证明的共识机制,让区块链中的各个节点贡献计算资源来寻找满足特定 SHA-256 哈希值对应的数值解,以维护区块链网络中资产所有权的唯一性。这个寻找随机数的过程类似矿工在茫茫矿区挖掘金矿,因而被俗称为“挖矿”。

共识机制是网络节点就数据或拟定交易的价值达成一致,并就此对账簿进行更新的机制,除工作量证明(PoW)外,还包括权益证明(PoS)、股份授权证明(DPoS)等[10]。以比特币的工作量证明机制为例,各节点基于计算机算力相互竞争来解决一个求解复杂但验证容易的数学难题,最快解决

该难题的节点将获得区块记账权和系统自动生成的比特币奖励[6]。A 与 B 的交易信息向全网络进行广播之后,所有权并不立即移转。网络节点将一定时期内未确认的新交易信息打包并进行工作量证明的计算,一旦某个节点找到符合要求的数值解,则向其他节点广播。其他节点接收并验证了哈希值,就会自动停止当前计算,并将接收的区块信息加入前序区块以更新所持有的账簿。A 以特定的 5 个比特币分别向 B、C 交易,若计算出有效哈希值的节点账簿中记有 A 与 B 之间的交易,则 B 取得这 5 个比特币的所有权,反之亦然,另一笔交易不发生所有权移转的效果。通过以上共识机制,使各网络节点确认并接收某一个获得特定区块记账权节点的账簿,并在其上继续记录和更新,从而保证了整个区块链系统中账簿的同一性。

在一些特殊的情形下,两个或多个节点同时完成了工作量证明,相互冲突的区块被链接至区块链末端,区块主链就可能会出现暂时的"分叉"现象。各节点会通过计算和比较,在各自认为有效的账簿后继续链接新区块,最终累积工作量证明最大化的那条区块链将被认为是唯一有效的,其余账簿则被回滚撤销[11]。数学上可以证明,当比特币网络中的一笔交易连续得到 6 个区块确认之后,回滚的概率即可忽略不计,此时 A 与 B 的交易才被不可逆转地记录到区块链账簿里。由于区块链系统内的每个节点都拥有一份完整的账簿拷贝,除非能够同时控制整个系统中超过 51%的节点,对任一节点的破坏或篡改均不影响其他节点的数据内容,被区块打包确认的交易信息因而能够被安全、永久和透明地记录下来。至此,A 与 B 买卖 5 个比特币的交易经过全网络广播,节点竞争记账权,6 次确认后最终实现所有权的移转。形象地说,区块链的这种分布式账簿相当于一个人人持有、集体维护,并实时记录着全部房地产交易和所有权变动的"房屋登记簿"。

区块链技术在无需第三方中心机构背书的前提下,真正实现了价值在互联网上的转移,被认为是可改变经济、金融和社会系统的革命性创新[12]。据报道,日本政府计划自 2018 年起将城市、耕地和林地等所有房地产和土地登记都统一到由区块链技术推动的单一账本上[13]。作为国家区块链战略的一部分,迪拜土地部门已开始使用区块链系统记录包括租赁登记在内的全部房地产交易,并与水电、通信系统相连[14]。在欧盟,一个利用分布式账本技术创建的增值税税收协议将于欧洲全境部署,从收据到银行存单,所有增值税会计交易会被纳入该系统进行统一处理。纳斯达克已上线用于私有股权交易的 Linq 平台,通过区块链技术进行数字化管理,有效降低资金成本与系统性风险。Ripple 公司利用区块链建立全球分布式支付清算体系,相比传统烦琐冗长的跨境支付流程,区块链可去除第三方中介环节,实现点对点的对接。国际支付巨头如 Paypal、Visa 等都相继开展了对区块链技术的探索和实践[15]。在国内金融业,中国建设银行携手 IBM 联合开发区块链银行保险平台,中国农业银行上线基于区块链的涉农互联网电商融资系统。腾讯、阿里巴巴等互联网巨头也纷纷布局区块链产业,力图打造企业级应用平台。

比特币作为区块链技术的最初应用,采用了一种相对简单的脚本代码来编程控制交易过程。通过锁定脚本和解锁脚本的组合,可为普通交易附加一定的条件,如延时支付、担保交易,多重签名等[6]。但是,比特币的脚本语言存在严重的限制,不具备图灵完备、不支持循环语句、不能获取区块链数据,一些复杂的交易因而无法实现。为提高脚本系统的灵活性和可扩展性,许多技术团队尝试在比特币协议之上进行改进或建立新的脚本协议,其中的佼佼者以超级账本(Hyperledger)、以太坊(Ethereum)等开源平台为代表。以太坊构建了图灵完备的脚本语言,让任何人都能够创建合约和去中心化应用,并在其中自由设定交易方式与规则。通过将合同内容以程序化规则和逻辑"翻译"成合约代码,并内置在任何区块链数据、交易及数字化资产上,合同条款就能够以按序、安全、可验证的方式自动执行。区块链为智能合约的实现提供了基础,智能合约则让区块链的应用延伸至金

融、法律和社会系统的每一个角落。

二、智能合约:自动执行的合同

(一)智能合约的定义与应用

智能合约的概念最早由学者尼克·萨博(Nick Szabo)于 1994 年提出,他认为智能合约是一套以数字形式定义的承诺(promises),并使用协议和用户接口来执行的合同条款。创造这一概念的初衷是希望通过将智能合约内置到物理实体的方式来构建各种灵活可控的智能财产,但由于技术手段的落后和应用场景的缺失,在当时并没有得到广泛重视。时至今日尚无一个关于智能合约的统一定义,许多论著是从密码学的角度以技术语言对其进行描述的。例如,将智能合约定义为部署在分布式账本上的程序代码,根据预先设定的条件管理数字资产[3]。其他的观点则将法学概念融入其中,认为智能合约是利用代码表现、确认和促进合同条款的自动执行[16]。或是通过电子方法控制资产所有权,以限制违约现象的产生[17]。在美国亚利桑那州通过的"区块链法案"中,智能合约被定义为:一个事件驱动的程序,可以在分布式、去中心化、可共享和可复制的账簿上运行,并且能够针对账簿中资产转移状况进行监管②。虽然以上定义的描述方式和角度不尽相同,但它们有一个共同点,就是都指明了智能合约与合同及区块链技术的某种联系。

在尼克·萨博的构想里,自动贩卖机是一个最简单的智能合约模型。当购买者投入特定数量的金钱时,自动贩卖机会按照预先设定的规则吐出相应商品。自动贩卖机通过物理密封的系统控制财产,以程序逻辑处理外部数据,从而实现了合同条款的自动执行。将自动贩卖机的概念无限扩大,智能合约就能依照特定协议内容自动移转房屋所有权、股权或知识产权。程序可以决定什么样的输入信息(inputs)符合合同履行的先决条件,如汇款、董事会成员投票或其他任何可通过代码表达的状态,因为程序逻辑中"if-then"的判断语句与合同履行具有天然的相似性。然而,将上述理论转化为现实有两大基本障碍:第一,计算机程序如何控制现实世界中的货币、股份等实物资产?自动贩卖机可以将商品封存于内部,传统的程序应用却难以提供安全可信的资产控制方式。第二,什么样的计算机系统或第三方机构能够不可篡改地存储和执行合约代码,并得到合同双方的信任?同时还需要在不对该计算机系统进行物理跟踪的前提下,能够保持最低限度的共享标准,以观察与验证其他合同当事人的执行记录[18]。

区块链技术的出现,有效解决了这些难题。区块链使完全数字化资产的移转成为可能,通过将价值以各种形式封包记录于区块之中,计算机代码就能够实现对资产权利的控制[19]。在区块链网络中,控制资产是指与控制资产对应的私钥,而不是任何实物。同时,区块链为智能合约的执行提供了一个安全可信的平台。一旦合约代码被写入区块链里,当事人可以确认合同条款被永久透明、不可更改地记录下来,并在约定的条件事项发生时自动触发合约的执行程序。在这个过程中,任何个人或机构都不能修改和删除合约,也无法阻止合约的自动执行,正如他们无法更改区块链中的数据信息一样。区块链成为为合约提供存储代码和状态的地方,再把执行合约的基本环境与一致性算法融合在一起,就构成了最基本的基于区块链的智能合约系统[20]。通过将合同内容进行数字化编码并部署在区块链上,让智能合约同样具有了区块链数据的一般特征,如分布式记录、存储和验证,不可篡改和伪造等。一旦完成部署,区块链即可实时监控智能合约的状态,并通过核查外部数据源、确认满足特定触发条件后激活并执行合同内容。

---

②Act of Mar. 29, 2017, ch. 97, 2017 Ariz. Sess. Laws, Ariz. Rev. Stat. § 44-7003.

简言之,智能合约就是部署于区块链上,可自动执行合同条款的计算机程序。区块链的技术特性能够保证合同的履行过程以一种去中心化、去信任、高度自治的方式进行,合同当事人无须信任彼此,因为嵌入分布式账簿中的合约代码使违约成本非常昂贵甚至无法实现。例如,互联网金融领域的股权众筹、P2P 网络借贷等商业模式可以借助智能合约实现,以避免传统模式中由网络平台等第三方机构进行资金募集、管理所导致的信用风险。该领域目前较为常见的是一种名为首次代币发行(Initial Coin Offering,ICO)的合约③。投资人向合约地址转账,智能合约会记录每一笔融资来源与金额,当达到特定融资额度时将自动计算并发放代表权利凭证的代币,当超过融资上限或融资失败时则原路退回资金。这一过程中,合同条款转化后的程序代码与交易的时间、对象及金额被永久透明地记录在区块链上,可供随时查看与验证。同时履约过程最大限度地排除了人为因素的介入,全程自动且无法干预,使合同利益能通过一种安全、去信任的方式实现。智能合约的以上特性,被认为是区块链技术扩大金融市场应用的关键因素[21]。

以比特币为代表的初级区块链应用,通常用于处理静态的数据记录或相对简单的交易逻辑。智能合约为区块链赋予了更灵活复杂的可编程脚本,以支撑各种典型行业场景的架构体系,故被称作"区块链 2.0"。目前,智能合约技术已被实验并应用于诸多领域,包括资产管理、数字票据、证券交易、清算结算、抵押贷款、供应链金融等。金融业务一般都具有标准化程度高、自动化需求大、信用度要求高等特点,因而和智能合约的优势高度契合。在以国际海运为代表的供应链金融领域,由于物流、资金流和信息流的复杂安排会涉及多份单据,且包括从当事人到银行、保险公司再到政府海关部门的众多主体参与,容易产生混乱和纰漏。各个主体之间往往缺乏沟通互信,难以建立一个统一透明的单据与交易管理系统,合同当事人又身处不同国家、地区,通过传统法律诉讼或仲裁的方式解决纠纷费时耗力。智能合约所具有的安全不可逆,公开透明且自动执行的特点,为供应链的每一个环节提供了更高的可跟踪性,并降低了其运营及信用成本。IBM、Everledger 等企业已开始将智能合约技术应用于该领域,以跟踪珠宝和中国猪肉产品[22]。

在未来,随着区块链技术的普及和完善,智能合约极有可能延伸至整个私法领域。例如,当房屋所有权登记系统被整合到区块链网络中时,房屋买卖合同就能以智能合约的形式加以实现。在特定房款汇入合约地址后,代表权利凭证的代币(token)会自动移转,如此可有效防止阴阳合同与过户纠纷。拥有房屋对应区块链资产的私钥才是真正的权利人,才能够进行有效的合约交易,夫妻共有等情形则可通过多重签名实现,从而避免了无权处分和无权代理的发生。区块链利用共识机制破解双重支付难题,也能用于应对房屋买卖中常见的"一房二卖"现象。智能合约是未来自动化、智能化社会的法律基石,将可能引发多个宏观社会系统的深度变革,包括众多私法领域内的既定规则。支持者声称"智能合约是法律系统的技术替代物,它无需任何现行法律规则就能够独立运作"[4]。或认为智能合约会"消除对合同法的需求,重塑商业交易流程和所有权机制",因为它"创造了一种超越法律界限的合同"[24]。这些言论无疑有过度夸大的嫌疑,从智能合约当前发展来看,它并未跳脱出现有的法学概念与框架。

(二)智能合约的法律构造

智能合约(smart contract)直译应为"智能合同",这一用语的言下之意表明它与传统合同具有某种联系,但又不完全相同。国外许多激进学者据此认为智能合约将取代传统合同[4],"由于它使合

③作为一种项目发起方募集资金的方式,ICO 类似于首次公开募股(Initial Public Offerings,IPO),但把所发行的标的物由证券变为了数字加密货币。

同的履行无法避免,因而改变了合同的本质"[23]。智能合约具有自动执行的特征,也被认为会在一定程度上替代法院强制执行的功能。另一些学者将智能合约与原合同分离,认为它是促进原合同履行的辅助手段,进而认定为是一种中介机制(escrow)或自助行为(self help)[24]。持反对意见的观点则否认智能合约的合同属性,认为它在很多情形下既不智能,也不合同。需要指出的是,智能合约一词首先是作为密码学和计算机术语提出的,在计算机语境下合约仅指部署于区块链中的程序语言,而不一定都具有法学意义上的内涵。正如 Stark 作出的区分,智能合约包括"智能合约合同"(smart legal contracts)和"智能合约代码"(smart contract code)双重含义[25]。智能合约由多段代码组成,但代码往往不能构成合同。下文所作分析,仅针对合同法角度的智能合约展开。

"新技术不一定会创造新的法学术语与原则,因为它们的基础构架往往没有根本性的改变"[26]。智能合约被称作是去信任的(trustless),意指智能合约对合同条款的自动执行,无须建立在对任何个体、法律规则或社会机构的信任之上,因为它本身即是建立信任的一种技术手段。有观点针对智能合约担保合同实现的功能,将其认定为类似信用证的独立担保工具[27]。信用证是一种银行开立的在一定条件下承诺付款的书面文件,是开证行应申请人的要求并按其指示,向受益人所签发的书面约定。根据这一约定,如果受益人满足了相应条件,开证行将向受益人支付信用证中约定的金额。信用证以银行信用代替商业信用,使交易双方可以无须信任彼此或其所属国家的法律系统而进行贸易往来[28]。除了常见的跟单信用证外,还有以担保债务履行为目的的备用信用证,在国内又常被称作银行保函、独立担保等④。智能合约作为一种去信任的履约机制,与信用证具有相似构造。智能合约通过对区块链资产的控制,以实现一定条件满足时的自动执行,正如同银行通过对账户资产的控制,以实现单证相符时的承诺付款。信用证是开证行与受益人之间的一种信用担保,它不借助任何物理实体而以银行独立无条件、第一位的见单付款作为担保义务。智能合约则是一种基于技术的信用担保,它以区块链公开透明、不可篡改的技术特性,保障了合同条款在约定条件下被安全可信地自动执行。

智能合约的本质,是在传统合同之上附加了一定的担保机制,这种担保不是透过私法工具而是由技术手段实现的。何谓担保?或提高优先性,或增加责任财产。智能合约通过将合同内容进行数字化编码并部署在区块链上,使合同指向的财产利益能得到确定移转,这就意味着当事人的债权能够先于普通债权人进行偿付,从而具有了事实上的优先性。在基于区块链的网络 P2P 借贷平台 Ethlend 中,借贷双方以智能合约的形式拟定并执行合同。借款人将具有一定价值的代币(token)打入合约地址,使智能合约能够控制其部分资产,贷款人再将借款打入合约。若借款人逾期未还款,合约中的 Erc20 代币或 ENS(Ethereum Name Service)域名将自动转入贷款人名下[29]。传统网络借贷往往在信用信息采集及核实、贷后跟踪、抵质押登记等问题上具有诸多困难,采用智能合约进行借贷则可有效避免相关风险,使贷款人的债权能够优先自动偿付。这种债权的优先执行不依赖于任何第三方机构或私法规则,而是以区块链不可篡改、条件满足时自动触发等特性为基础,使全球化的网络借贷市场成为可能。

一般认为,信用证或独立保证具有两大典型特征。第一,独立抽象性。开证行作出兑付、议付或履行信用证项下其他义务的承诺,不受申请人与开证行之间或与受益人之间在已有关系下产生的索偿或抗辩的制约⑤。信用证是一种"先付款,后争议"(pay first, argue later)的交易工具,在开证

---

④信用证与独立保函、独立担保、独立保证等概念没有本质区别。参见高祥《论国内独立保函与备用信用证在我国的法律地位——兼评最高人民法院独立保函司法解释征求意见稿》(《比较法研究》),2014 年第 6 期)。

⑤Uniform Customs and Practice for Documentary Credits (UCP600), Article 4.

行付款后若发现履行不符合要求,只能根据基础合同请求赔偿。智能合约的情形同样如此,被写入区块链中的交易无法更改,触发条件满足时,合同约定的履行条款便会被永久不可逆地执行。围绕原合同的若干争议,如合同无效、可撤销、不完全履行等,只有通过原合同加以解决。第二,单据性。开证行处理的是单据,而不是单据可能涉及的货物、服务或履约行为⑥。通过将付款条件单据化,开证行可以直接通过受益人提交的单据与信用证条款是否相符进行判断,无需再就基础交易的履行情况作进一步调查。智能合约则将付款条件代码化,仅根据预先设定的程序逻辑对特定外部信息加以回应,未被定义的外部信息无法影响合约状态,以保证带有触发条件的数字化承诺能按照当事人的意志执行。

智能合约与信用证同为基于信任的担保机制,在结构上具有一定相似性,但两者又不完全相同。信用证将完整合同的部分内容抽离出来,只对该部分予以担保,这也是其独立性和单据性特征的由来。例如,跟单信用证担保的是货款支付,一般要求卖方提供商业发票、保险单和装船清洁提单等。这就意味着跟单信用证仅对基础合同中的主义务、保险义务、运输义务予以担保,其余条款的内容则不在担保范围以内,基础合同的各项抗辩权也不会影响信用证的效力。智能合约将基础合同的全部内容转化为机器语言,在理想情况下,任何可能改变合同履行状况的条款都被写入程序代码之中。因此,智能合约的担保范围比信用证更为宽泛,能够覆盖基础合同的全部条款。在现实世界,一个审核与监督合同完整生命周期并担保其履行的第三方机构无法存在,因为这会承担非常高的风险和极端昂贵的运行成本。智能合约由分布式的集体维护,可编程脚本控制状态,使全合同的担保执行成为可能。随着人工智能、物联网技术的发展完善,智能合约将有可能突破独立性原则,成为一种全新的担保方式。

除担保功能外,智能合约还是基础合同的数字化载体。智能合约需要将原始合同通过编程语言转化为合约代码,再广播至区块链网络中,因而它本身亦是表现和存证原始合同的载体。这种存证功能分为两种形式:其一,作为要约的形式。从初始的智能合约模型——自动贩卖机,到实践中得到广泛应用的 ICO 合约,都是一种以订立合同为目的须受领的意思表示。当购买者投入硬币、投资人向特定合约地址转账后,得依承诺或意思实现成立合同,智能合约仅具有要约的内涵。其二,作为合同的形式。当事人预先拟定原始合同,或直接以程序语言进行编写。无论哪一种情形,智能合约均能够表征基础合同的相应内容,它本身也可被视作以数据电文形式订立的合同。因此,智能合约包括“要约+独立担保”“合同+独立担保”两种法律构造,它没有改变合同的本质,而是在合同或要约之上添加了辅助履行的担保功能。通过技术手段控制区块链资产,以实现条件符合时合同条款的自动执行,使债权人获得了事实上的优先地位。在未来,各类资产逐步数字化,成为链上资产后,智能合约的应用空间将更为广泛与深刻。

(三)智能合约的风险与挑战

尽管区块链与智能合约的前景广阔,但其当前发展仍处于初级阶段,从技术角度而言远未达到可以广泛应用的程度。2016 年,时称史上最大众筹项目,基于以太坊的去中心化组织 The DAO 遭到黑客攻击,由于 The DAO 智能合约自身的漏洞,导致约 6 000 万美元流失。DAO 意为去中心化或分布式自治组织(DAO, decentralized autonomous organization),指完全由智能合约控制投资和运行的公司实体,持股人通过链上投票而非中心化的管理部门来决定公司的活动[30]。攻击者针对 The DAO 合约中包括递归调用(recursive calling)在内的多个漏洞进行攻击,并向一个匿名地址转移了

⑥Uniform Customs and Practice for Documentary Credits (UCP600), Article 5.

360 万个以太币,约合其众筹总量的 1/3。最终 The DAO 团队宣布辞职,并被迫解散了项目。然而该事件发生后现有法律规则如何适用疑点重重,DAO 是否属于公司法意义上的企业法人? 合约漏洞是否构成违约或侵权? The DAO 项目方又应当负有何种责任? 种种问题至今未有定论,鉴于法律救济上的困难,以太坊社区最终选择了使用技术手段即所谓的"硬分叉"作为解决方案。

智能合约被称为是安全可信,不可篡改的,意指智能合约在合同履行过程中最大限度地减少了人为干预,但这并不意味着合同能被确保圆满执行。在大多数情形下,智能合约不仅是简单的区块链交易,还是运行于其上的条件式代码。当合同的履行状况与代码相关联时,就不可避免地受编码错误(coding error)的影响,因为任何计算机程序都有可能产生漏洞。不可篡改、自动执行的特质仅仅使其排除履约过程中人为因素的介入,但同时又引入了新的风险,即合同的履行可能因代码漏洞出现瑕疵甚至无法进行[31]。由于智能合约通过数字化合同标的并控制其移转,代码漏洞会导致标的灭失以致履行不能,所谓智能合约能够规避违约的论点也就无法成立。在 DAO 事件中,项目的本旨类似于风险投资基金,但因合约中的资金被盗致使合同无法继续履行。这种漏洞可能由当事人、第三人,或多方共同引起,因而有意思表示错误、欺诈及侵害债权等私法规则的适用余地。无论如何,智能合约并非完全杜绝了合同中的人为因素,只是将其从履行阶段提前至合同订立阶段,各类影响合同利益实现的情形仍有可能发生。

在合同订立过程中,不仅最终成型的合约代码可能存在漏洞,机器语言的转化也可能扭曲或丧失合同真意。传统合同一般由自然语言或法律语言书写,通过计算机程序执行合同条款则首先需要将其转化为机器语言。对于现有技术水平而言,尚无法将这一过程自动化为人工智能或机器学习手段,除非是在大幅减损转化质量的情况之下[32]。而在很多情形,即使智能合约的功能性没有技术上的缺漏,它也无法准确反应和表示合同的原始内容。例如,现代商业合同往往需要使用大量模糊的词句以达到特定目的,对于"甲方应尽最大努力完成合同义务"等类似的表达就无法通过机器语言进行描述。合同的模糊性是一种功能而非缺陷,它在提高争议可能的同时也增加了合同的灵活性和柔韧度,使当事人能够根据现实情形的变化作出细微调整而无需重新缔结合同。智能合约的代码要求将自然语言转化为条件语句,这就意味着全部合同条款都被翻译成若 A 即 B 的形式,像"合理注意"或"最大努力"等难以准确评价行为内容及结果的用语则无从适用。

被称为能预防违约的智能合约,还需要在订立之初就对合同生命周期中可能发生的全部情形进行准确预测。如果智能合约对合同履行阶段进行完全控制并排除人为干预,那么任何可能改变履行状况的事件都应被提前写入代码之中,否则自动执行将沦为一纸空谈。在自动贩卖机的场合,由于涉及的法律关系是简单的买卖合同,所有可能发生的履约情形都能够被简单的计算机逻辑所囊括。但对于复杂的商业合同而言,市场环境瞬息万变,往往需要使用非确定性的语句对未来状况及合同权利义务予以描述,试图在一开始就精确预测与分配违约责任几乎是不可能完成的任务。智能合约试图扩大应用的前提是任何合同条款都可以被条件式代码所翻译和覆盖,然而这与现实世界的交易事实相背离。从目前实践来看,绝大多数基于智能合约的应用平台(如借贷、支付等)都使用了预先设定的代码范本,仅允许用户在少数变量上进行修改。定型化的合同类型减轻了代码编写的专业化要求,降低了履行变量的预测难度,但同时也使智能合约当前的应用形态更接近格式条款,而非完整合同。

对于现有技术水平而言,智能合约也很难实现与链下实物的交互。区块链的设计对象是完全的数字环境,无法直接接收来自现实世界的信息输入。技术上区分链上(on-chain)与链下(off-chain)两种信息源,时间序列、区块信息、代币移转等属于链上事件,其余全部物理实体和活动都属

于无法被区块链原始识别的链下事件。例如,特定时间的金融数据就不能被区块链网络直接获取,而需要通过名为预言机(Oracle)的数据源加以引入,再由智能合约验证条件并触发交易或更改状态。然而预言机既不是去中心化也非去信任的,并不能保证链下事件的真实发生以及数据的准确性,往往需要当事人事先就采纳特定预言机达成一致,如此就大幅削弱了智能合约的可靠性[33]。链下事件分为公开数据事件和非公开数据事件,后者如特定快递的送达情况就难以被一般数据源感知,只有借助传感器及物联网技术才能写入区块链网络中,但这些技术离广泛应用还很遥远[34]。具有主观标准的合同标的也难以转化为计算机数据,无法被预言机所认知和评价,链下事件驱动的自动执行也就无从实现。因此,当前几乎全部智能合约应用都集中在链上的虚拟环境中,对于延伸至链下的应用场景仍有相当距离。

基于区块链的智能合约技术还具有一定程度的监管风险。2017 年 9 月 4 日,中国人民银行等七部委联合发布《关于防范代币发行融资风险的公告》,将 ICO 合约定性为非法融资,“涉嫌非法发售代币票券、非法发行证券以及非法集资、金融诈骗、传销等违法犯罪活动”,要求“各类代币发行融资活动立即停止”。然而 ICO 合约的通用平台是基于公有链的以太坊网络,全球任何地区都可以设立合约或参与募集资金,这就使特定国家的强行法规难以有效限制合约的履行。大量国内项目在公告发布后通过包装换皮,转移至其他地区重新开展代币发行活动。据统计,2018 年前 3 个月的 ICO 月募集量均超过 1 亿美元,是 2017 年 9 月的 2 至 3 倍,其中不乏大量出海的国产项目。由于区块链具有跨国跨地区传输价值的特性,使智能合约能够面向全球不特定地区与人群进行合同的要约、订立及履行,这就让传统的准据法规则难以适用,单一国家的私法构架和强行命令也会被刻意绕开。区块链网络虽然记录了全部交易及合约历史,但合约的现实拥有者却很难查证,这也为洗钱、恐怖犯罪活动等提供了滋生的温床。

与将其捧上神坛的结论不同,智能合约并非是能解决一切合同履行问题的万能钥匙,这些观点通常都忽视了它的法律及技术瓶颈。比特币作为最初的区块链网络是安全去信任的,但同时也极度限缩了交易的灵活性与范围,更复杂的合同类型需要更复杂的区块链底层协议,而这些协议往往牺牲了去中心化,安全透明等特性。如此,区块链原有的优点在智能合约中将可能不复存在。智能合约还具有编码漏洞、语言转化、现实交互、跨国监管等诸多风险与挑战。因此在当前及未来很长一段时间内,智能合约的应用领域仍将集中在简单、定型化的合同类型及虚拟场景中,对于进一步扩大化应用需要法学及技术角度的共同挖掘与探索。

三、结语

区块链被称为第四次工业革命的发动机,是具有普适性的底层技术框架,它不仅与民法息息相关,更有可能深刻改变传统私法领域的既定规则。区块链使用了独特的方式对现实世界交易流程进行模拟,因而能被民法原理所解读,并加以拓展和运用。在其之上建立的智能合约技术,被认为可能引发金融、法律活动的深度蜕变,通过将合同内容进行数字化编码并部署于区块链上,使合同的履行过程能够以去一种中心化、去信任、高度自治的方式进行。然而许多观点过度夸大了智能合约的功能,将其比作法律系统的替代物,或认为它能永久消除违约。实际上,智能合约并未超越现有的法学概念,它的实质是运用技术手段在合同或要约之上添加了辅助履行的担保功能,使合同指向的财产利益能得到确定移转。从现有发展来看,区块链及智能合约技术尚处于初级阶段,主要应用都集中在定型化的虚拟场景之中,离广泛而全面的普及仍有一定距离。智能合约还具有多重法律及技术瓶颈,在诸如编码漏洞、语言转化、现实交互、跨国监管等问题上存在一系列风险与挑战。

在未来,随着区块链与智能合约技术的革新和进化,将为法学领域带来何种冲击,现有私法规则又将如何回应,值得进一步探讨与深思。

参考文献:

[1]NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[R/OL].(2008)[2018-03-15].https://bitcoin.org/bitcoin.pdf.

[2]European Parliamentary Research Service.How blockchain technology could change our lives[R].EPRS,2017.

[3]BUTERIN V.Ethereum: A next-generation smart contract and decentralized application platform[R/OL].[2018-04-01].https://github.com/ethereum/wiki/wiki/White-Paper.

[4]SAVELYEV A.Contract Law 2.0:'Smart' contracts as the beginning of the end of classic contract law[J].Information & Communications Technology Law,2017,26(2):116-134.

[5]SCHROEDER J L.Bitcoin and the uniform commercial code[J].SSRN Electronic Journal, 2015.

[6]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):482.

[7]KIVIAT T I.Beyond Bitcoin:Issues in regulating blockchain transactions[J].Duke Law Journal,2015,65:569-574.

[8]GRAY J.IBM res.laboratory,notes on data base operating systems[R].Lecture Notes In Computer Science,1978:394-465.

[9]PEASE M,SHOSTAK R,LAMPORT L.Reaching agreement in the presence of faults[J].Journal of the Association for Computing Machinery,1980,27:228-234.

[10]KPMG.Consensus:Immutable agreement for the Internet of value[R/OL].(2016-09-19)[2018-06-26].https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2016/09/blockchain-consensus.pdf.

[11]ANTONOPOULOS A M.Mastering Bitcoin:Unlocking digital cryptocurrencies[M].O'Reilly Media,2014:206.

[12]TAPSCOTT D,TAPSCOTT A.Blockchain revolution[M].Penguin,2016:105.

[13]Nikkei.Japan to tidy up scattered property records[EB/OL].(2017-06-14)[2018-06-20]. https://asia.nikkei.com/Markets/Property/Japan-to-tidy-up-scattered-property-records.

[14]DAS S.100%: Dubai will put entire land registry on a blockchain[EB/OL].(2017-10-09)[2018-07-11]. https://www.cryptocoinsnews.com/100-dubai-put-entire-land-registry-blockchain.

[15]唐文剑,吕雯.区块链将如何重新定义世界[M].北京:机械工业出版社,2016:115-152.

[16]SWANSON T.Great chain of numbers:A guide to smart contracts,smart property,and trustless asset management[M].Kindle, 2014:11-16.

[17]SZABO N.Formalizing and securing relationships on public networks[J].First Monday,1997,2(9):1-21.

[18]STARK J.How close are smart contracts to impacting real-world law[EB/OL].(2016-04-11)[2018-07-20]. https://www.coindesk.com/blockchain-smarts-contracts-real-world-law.

[19]ATTA-KRAH K D.Preventing a boom from turning bust[J].Iowa Law Review,2016,101:1187-1222.

[20]胡凯,白晓敏,于卓.智能合约工程[J].中国计算机学会通讯,2017(5).

[21]PINNA A,RUTTENBERG W.Distributed ledger technologies in securities post-trading revolution or evolution? [R].European Central Bank Occasional Paper,2016,172:18.

[22]CHAMBER OF DIGITAL COMMERCE. Smart contracts:12 use cases for business & beyond[R].2016:32.

[23]WERBACH K,CORNELL N.Contracts ex machina[J].Duke Law Journal,2017,67:28.

[24]RASKIN M.The law of smart contracts[J].SSRN Electronic Journal,2016.

[25]CLACK C D,BAKSHI V A,BRAINE L.Smart contract templates:Foundations,design landscape and research directions[J/OL].(2016-08-02)[2018-07-28].http://arxiv.org/abs/1608.00771.

[26]EASTERBROOK F H.Cyberspace and the law of the horse[R].University of Chicago Legal Forum,2015.

[27]MCJOHN S M,MCJOHN I.The commercial law of Bitcoin and blocktrain transactions[J].Suffolk University Law School Research Paper,2016:13.

[28] MCJOHN S M. Assignability of letter of credit proceeds: Adapting the code to new commercial practices[J]. Uniform Commercial Code Law Journal,1993,25:257-271.

[29] ETHLend.Io white paper democratizing lending[R/OL]. (2018-02-25)[2018-08-24]. https://github.com/ETHLend/Documentation/blob/master/ETHLendWhitePaper.md.

[30] RASKIN M. The law and legality of smart contracts[J]. Georgetown Law and Technology Review,2017,1:305-341.

[31] BAMBERGER K A. Technologies of compliance: Risk and regulation in a digital age[J]. Social Science Electronic Publishing,2010,88.

[32] SURDEN H.Machine learning and law[J].Washington Law Review,2014,89(1):87-115.

[33] ZHANG F,CECCHETTI E,CROMAN K,et al.Town crier: An authenticated data feed for smart contracts[R].The 23rd ACM Conference on Computer and Communications Security,2016:1.

[34] SHAY L A,HARTZOG W,NELSON J,et al.Confronting automated law enforcement[M]//CALO R,FROOMKIN M,KERR I.Robot Law.Edward Elgar Publishing,2016:235-273.

Civillaw analysis, application and enlightenment of smart contract under blockchain technology

NI Yunwei

(*Law School*, *Nanjing University*, *Nanjing 210093*, *P. R. China*)

Abstract: Blockchain, known as the engine of the fourth industrial revolution, is a universal framework of underlying technology. It is not only closely related to civil law, but also more likely to change the established rules of traditional private law. Blockchain simulates the real world trading process in a unique way, so it can be interpreted by the principles of civil law, and be expanded and applied. The smart contract technology built on it is believed to lead to deep transformation of financial and legal activities. By digitizing the content of the contract and deploying it on the blockchain, the execution of the contract can be carried out in a decentralized, trustless, and autonomous way. However, smart contract does not surpass the existing legal concept. Its essence is to add collateral function on the contract or the offer by technical means, so that the property interests directed by the contract can be transferred. For the current level of development, blockchain and smart contract technology are still in the early stage, most of the applications are concentrated in the stereotyped virtual scene, and there is still a certain distance from comprehensive popularization. Smart contracts also have multiple legal and technical bottlenecks, and there are a series of risks as well as challenges in such issues as coding loopholes, language transformation, reality interaction, transnational supervision and so on.

Key words: blockchain; smart contract; Bitcoin; Ethereum; contract law

(责任编辑　胡志平)