保险智能合约的法律构造与风险防控

赛 铮*

摘要: 保险智能合约是完全自动化执行的合同,呈现出“代码即法律”的构造方式:在合约成立时表现为代码,合约有效表现为区块链验证,合约执行表现为自动执行软件。保险智能合约能够实现理赔处理的自动化,减少人为干预,缩短理赔时间,未来具有广阔的应用前景。作为代码合同的保险智能合约可能存在代码漏洞、代码瑕疵,具有单一封闭性,“去中心化”监管与传统监管理念冲突等法律风险。在智能合约与保险相结合的发展趋势下,应当以科技治理为逻辑线索,从科技治理蕴含的“技术驱动”“多元协同”以及“一般原则与特殊工具的统一”等层面,构建“技术规范—机制设计—智能监管”的具体法治路径。

关键词: 区块链 保险智能合约 法律构造 法律风险 科技治理

一、问题的提出

当下,区块链技术已成为全球金融创新的热点方向,作为金融业之一的保险业也不例外,区块链技术在保险业中的应用趋势已逐渐显现。^① 目前区块链技术的实施领域之一是完全自动化的合同——智能合约,即在信息技术环境中,智能合约自动执行。保险智能合约是其中的一种类型,具体指一段根据传统保险合同编写的软件代码,在区块链平台上执行,从而确保保险智能合

* 桂林电子科技大学法学院副教授

基金项目:广西省哲学社会科学基金资助项目(22CFX005)

^① 现阶段区块链技术在保险行业的应用主要集中在产品开发、流程优化和再保险平台建构等领域。在产品开发与流程优化方面,如中美联泰大都会人寿保险有限公司的“生命链”(Lifechain),是基于智能合约的人身保险理赔服务平台,可帮助死者的家属和亲人便捷和快速地确认相关保单情况:是否属于保险责任范围、理赔条件和要求,并自动提出理赔申请。安盛天平财产保险有限公司的“以太坊公有区块链航班延误保险产品”(Fizzy),为航空旅客提供自动航班延迟赔偿,当航班延误超过2小时,赔偿机制将会自动执行,直接发送至投保人的信用卡账户中,独立于安盛天平财产保险有限公司的决定。在再保险平台建构方面,主要有英国保险科技初创公司的“区块链再保险解决方案”,以及由原中国银行保险监督管理委员会上海监管局牵头,众安在线财产保险股份有限公司、德国通用再保险股份有限公司、汉诺威再保险股份有限公司等共同参与的“区块链再保险试验平台”等。

约条款的自律性和自主性,这些条款由事前设定的保险合同条件触发,并应用于区块链的资产中。这一特征刚好与保险业中所尊崇的最大诚信原则的经营前提相契合。“区块链提供的算法信任,不仅给社会信任体系的重构以可能,也给了保险经营管理模式,乃至整个业态的存在以新挑战和新机遇。”^①保险智能合约能够实现理赔处理的自动化,减少人为干预,缩短理赔时间,减少理赔纠纷,有效解决当下我国保险合同纠纷已然成为保险投诉“重灾区”的困境。^②因此,保险智能合约未来存在广阔的应用空间。但是,目前学术界对保险智能合约的法律构造并没有明确的界定,导致后续保险智能合约应用过程中的风险防控手段也付之阙如。申言之,保险智能合约与传统保险合同相比其法律构造有何特征?保险智能合约的使用会对法律产生什么样的风险?保险智能合约产生的风险应如何防控?有鉴于此,笔者尝试运用法学和区块链的原理,阐释内嵌于区块链技术中的保险智能合约的法律构造,以保险智能合约向传统合同提出的数字化挑战和法律风险为问题导向,探讨如何从科技监管的视角,基于“科技治理”的理论,为保险智能合约引发的法律风险提供有效的防治路径,以保障金融创新与金融安全之间的动态平衡。

二、保险智能合约的法律构造

作为一项从密码学和信息科学延伸而来的技术,区块链保险智能合约与传统保险合同有较大区别,保险智能合约是由代码编写而成的合同,其“成立—有效—执行”的过程全部由代码在区块链中加以实现,构成了“代码即法律”的新型合同形式。

(一) 合约成立:编写代码

保险智能合约得以成立,首先需要投保人与保险人之间通过要约承诺彼此达成合意,确立权利义务关系后,由编程人员将彼此的权利义务从自然语言转化为机器语言,即代码。

1. 保险智能合约的成立是依靠代码实现的。智能合约是一段代码,存储在区块链上,由区块链交易触发,并在该区块链数据库中读取和写入数据,该代码不可篡改且自动执行。“代码是互联网体系结构的基石,因此它有能力通过技术手段规范个人行为。”^③基于私法的“合同自由”原则,由代码体现的智能合约得以存在并推广应用。保险智能合约通常采取格式合同的形式,最典型的执行代码语言是“如果 A,那么 B”。保险智能合约事先设定好的条件一旦触发,将会自动执行。此外,保险智能合约的成立仅以代码编程的电子形式存在,不可能使用任何其他形式的合同(如口头、书面等形式)。

2. 代码使保险智能合约增加了确定性与信用度。就确定性而言,保险智能合约的核心是代码,其实质是一种具有严格定义语义和语法的计算机语言。代码的逻辑语言可以通过将交易双方的承诺转变为客观可验证的技术规则从而使合同内容变得确定。在传统合同中,合同术语

^① 王和:《保险的未来》,中信出版集团股份有限公司2019年版,第31页。

^② 据中国银行保险监督管理委员会办公厅统计,2018年中国银行保险监督管理委员会及其派出机构共接受涉及保险公司的保险消费投诉88454件,其中,保险合同纠纷投诉86491件,占投诉总量的97.78%。参见《中国银保监会办公厅关于2018年度保险消费投诉情况的通报》,https://www.gov.cn/zhengce/zhengceku/2019-11/11/content_5450876.htm,2019-11-11。

^③ [美]Primavera De Filippi, Samer Hassan:《从“代码即法律”到“法律即代码”——以区块链作为一种互联网监管技术为切入点》,赵蕾、曹建峰译,《科技与法律》2018年第5期。

的解释由人脑基于主观标准和思维方式来执行,不可避免地存在模糊性。而代码的确定性能有效化解这一问题。尽管代码编程语言中也可能存在模糊性,但这些模糊性比现实世界中自然语言引发的模糊性要小,因为计算机可识别的术语比人类自然语言可识别的术语少得多。^①就信用度而言,保险智能合约高于传统合同。一方面,信用度高是因为区块链中的代码是透明的,用户随时可对其进行查看。另一方面,信用度还同程序员提供给程序处理的数据有关。数据真实性越高,关联性越强,那么智能合约的信用度就越高。因此,数据的真实性与关联性也至关重要,而区块链的技术特征很好地为数据的真实性与关联性提供了保障。^②

3. 代码体现保险智能合约中的各项功能。在代码编程设计中,保险智能合约在保险服务器中创建。在创建期间,代码提供附加信息并将其存储在合同上,如合同生效后的持续时间和安装在车辆上的电子设备的地址。在创建过程结束时,代码会为已编写的智能合约分配一个地址,以便将来进行自动交易。一旦保险消费者从个人钱包(为智能合约提供资金)进行交易,就会调用代码函数。该功能识别保险消费者(即顾客钱包的地址)将该信息存储在智能合约上作为保险智能合约的签订人和未来退款的接收者。此外,该功能还记录合同激活时间。保险人将私钥交由保险消费者管理,保险消费者的密钥存储在电子设备中,此种模式能增加系统的安全性,即便在“黑客”攻击保险智能合约系统的情况下,也仅只有所有者的钱包(具有有限的余额)会受到损害,从而最大限度地降低风险。^③

(二) 合约有效:区块链验证

在传统合同中,交易双方达成一致合意后,还需要经过法律的评价才能确定其是否能够成为受法律保护的对象,即根据合同是否违反法律强制性规定以及是否违反公序良俗而判定其效力。在智能合约中,同样也存在合同有效性问题,但智能合约的有效性不是基于法律规定,而是须经过区块链的各节点验证后方可生效。

1. 智能合约成立的代码需要发布到区块链上,才能成为真正意义上有效的智能合约,即条件触发时能够自动执行。通常智能合约发布者通过点对点网络协议建立无中心的网络通信拓扑(用传输介质互连各种设备的物理布局),拓扑中每个节点在参与智能合约记录的同时,也负责验证其他节点记录结构的正确性,并借助约定的共识协议机制,保证只有全网大部分节点都认证该智能合约记录正确时,其真实性才算得到全网区块链认可。例如,在盗窃、火灾事件的保险智能合约激活期间,被保险人需要拍摄车辆的若干张照片,包括车辆正面、背面、两侧和顶部的照片等,照片中的车辆须显示车牌。保险人提醒顾客在光线充足的地方拍照并避免图片失焦。拍摄完每张照片后,移动应用程序会将其转换为十六进制字符串并将其发送到电子设备上。电子设备运用算法计算十六进制字符串的排列,通过代码函数存储在智能合约中,该函数还记录保险合同相关的保险金和时间戳,作为给定时间图片的存在证明。此外,区块链上的所有节点都可以验证该证明是否真实准确。

^① See Alexander Savelyev, *Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law*, Basic Research Program Working Papers, 2016, p. 13.

^② 参见徐忠、孙国峰、姚前主编:《金融科技:发展趋势与监管》,中国金融出版社2017年版,第9页。

^③ See Lamberti F, Gatteschiv, Demartini C, et al. *Blockchains Can Work for Car Insurance: Using Smart Contracts and Sensors to provide on-demand Coverage*, 7 (4) IEEE Consumer Electronics Magazine, 72 (2018).

2. 智能合约一旦在区块链上经过验证后就变成有效代码,包括保险人与被保险人在内的任何人都无法篡改。即区块链已完成验证,在各节点中产生新块(新的分类账),共识固化。依靠签名技术,区块链使得每一个操作都可鉴权(验证用户身份)可审计;依靠哈希链式数据结构使得所有的数据融为一体,无法单独修改其中的任何一点;通过共识算法,可以让所有节点形成合力。除非对区块链上的节点数量控制超过一定阈值(通常为 51%),否则对区块链上个别节点数据进行更改是不可能的。^① 保险智能合约一旦经过区块链验证后生效便无法篡改,当智能合约的条件被触发时,由区块链自动执行,合同交易双方不能依自己的意志进行阻拦。

(三) 合约执行:自动软件

智能合约生效后,一旦条件触发便自动执行。即保险智能合约的执行是自动化的,全程不再有人为干预。设定的条件触发后,经过区块链验证,代码即自动运行。在触发条件的验证中,若保险智能合约设定的赔付条件满足时,区块链各节点将保险人账户中锁定的金额支付给被保险人。若赔付条件不满足时,保险人账户中锁定的金额不发生变化。合同执行的全过程不再依赖于人的中介,而人的中介可能会因主观原因或过大的自由裁量权造成保险理赔纠纷。在保险业中,智能合约的应用能极大提高保险理赔的效率,更好地服务于保险消费者。例如,在航空延误险中,通过保险智能合约的自动软件执行,当航班延误超过设定的若干时间时,保险智能合约自动将延误赔偿金转入被保险人的账户,整个过程保险公司无法介入和干预。智能合约在执行过程中不需要包括合同当事人、相对人及第三人等任何民事主体的介入,换言之,保险智能合约一旦上链成功,便成为一种默认、强制且不可逆的合约。

综上所述,保险智能合约是“代码即法律”的构造形式,基于区块链技术的保险智能合约缔约、履行过程可以简化表述为以下 3 个步骤:(1) 合约成立,即参与缔约的双方或多方当事人商定后将共同合意编写成一份代码表示的智能合约;(2) 合约有效,即将智能合约内容发布至区块链,验证节点通过后产生新块,并存储于区块链各节点中;(3) 合约执行,即存储于区块链中的智能合约一旦触发执行条件,经过各节点验证通过后便不可逆地自动执行合同内容。^②

三、保险智能合约蕴含的法律风险

保险智能合约是存储于区块链各节点中的一段代码,根据代码编写的条件触发后自动执行。区块链智能合约既是代码技术,同时又是法律合同,亦反映合同当事人交易的变动与调整,对当事人的权利义务产生约束。保险智能合约的代码属性对传统合同法提出了数字化、单一封闭性以及去中心化的挑战。

(一) 三元结构的传统合同向四元结构的代码合同转型

合同是反映交易的法律形式。我国法律将合同定义为一种协议。^③ 长期以来,当事人采用书面或口头形式订立合同,通常其合同成立是由“要约人—承诺人—协议”的三元结构组成。在

^① 参见杜宁、王志峰、沈筱彦等:《监管科技:人工智能与区块链应用之大道》,中国金融出版社 2018 年版,第 162 页。

^② 参见夏沅:《区块链智能合约技术应用》,《中国金融》2018 年第 6 期。

^③ 参见《中华人民共和国民法典》第 464 条第 1 款。

保险智能合约中,其本质是写入区块链中的一段代码,该代码不可篡改且自动执行。这使得传统合同的三元结构发生了重大转变,转向“要约人—承诺人—协议—代码”的四元结构。传统合同由交易当事人之间的一致合意构成,合同的执行围绕双方的意志展开,智能合约则反其道而行之,其自动执行的特征使得合同交易方的意志有别于传统合同的形式。^① 简言之,保险智能合约是合同与代码的结合,合约由代码表示,并由代码自动执行。智能合约的编码不是由银行、保险公司等机构根据协议条款实现财产的数字转移,而是自动完成所有工作。区块链上的“矿工”(区块链网络的参与者)只需决定协议的内容,合同就能有效执行。智能合约通过允许区块链处理交易所有内容,使合同交易减少人为干预实现去中心化,从而提高效率。^②

然而,保险智能合约作为内嵌于区块链的代码合同,不可避免地会存在代码风险。(1)代码漏洞。区块链是一种将数据区块按时间顺序相连接组合而成的块链式数据结构,并以密码学方式保证的不可篡改和不可伪造的分布式账本。^③ 区块链属于算法高频率、高密度的技术,存在代码漏洞的安全隐患。“随着计算能力的不断进步,这些机制的基本弱点更加难以消除。”^④一旦密码被“黑客”破解,或存在高级别的漏洞,将带来巨大负面影响,甚至使整个区块链大厦轰然倒塌。除了人为原因外,使用大量加密算法的区块链在运行中的缺陷是客观存在的,毕竟能将保险合同完全适配于区块链技术的专业人士现阶段还十分稀缺。(2)代码瑕疵。代码语言相较于自然语言简单得多,代码编写的智能合约在实施过程中很难与人的真实意志完美对应。首先,代码的编写需要专门的技术,仰仗于专业的计算机人员对合约自然语言的理解能力,这个过程不可避免地会存在主观判断、解释和决策等因素。若计算机人员在对合约进行编写代码的过程中存在理解偏差,那么该智能合约在一定程度上将掩盖或扭曲合同交易双方的真实意志。简言之,这是简单代码与复杂语言之间的冲突。其次,现实世界中交易双方的权利义务关系通常是复杂的,有时由于在签订合同的过程中尚有一些要求难以确定,因此双方会约定部分开放性或兜底性的条款,以此来解释未来可能存在的变化。但是,由代码编写而成的智能合约在现阶段还不具备承载此种内容的合约安排。最后,代码编写专业人才短缺也会衍生很多问题,如现阶段的智能合约升级困难,发现漏洞时,很难通过升级的方式来解决。^⑤

(二)合同性质由开放属性向单一封闭属性转变

传统合同具备开放性,此处的开放性指的是合同签订后往往可进行变更、解除、撤销等。而保险智能合约一旦写入区块链中,编写的代码是按照“成立—生效”的逻辑执行,在区块链上发生的传输是即时的,随着分布式记账技术和智能编程的进一步完善,即使是最复杂的交易,也可以实现即时结算,故而智能合约具有单一封闭属性。具体而言:

1. 保险智能合约一旦成立即生效。传统合同成立关注的重点在于双方当事人之间是否经由要约承诺达成一致合意,而合同效力是否产生是由合同法加以规制,当事人通常并未关注。换

^① 参见王延川:《智能合约的构造与风险防治》,《法学杂志》2019年第2期。

^② See Mark Giancaspro, Is a Smart Contract Really a Smart Idea? Insights from a Legal Perspective, Computer Law & Security Report, 2017, p.4.

^③ 参见曹源、张翀、丁兆云等:《DAG区块链技术原理与实践》,机械工业出版社2018年版,“序三”第4页。

^④ [美]凯文·沃巴赫:《信任,但需要验证:论区块链为何需要法律》,林少伟译,《东方法学》2018年第4期。

^⑤ 参见徐忠、孙国峰、姚前主编:《金融科技:发展趋势与监管》,中国金融出版社2017年版,第20页。

言之,若合同违法,则哪怕合同已成立,也不发生法律效力。^① 然而,智能合约使得合同发生效力的过程不再是成立与生效两个阶段,其“代码即法律”的构造使得合约一旦编成代码并发布在区块链中,条件触发便自动执行,这意味着智能合约成立的同时即已经发生法律效力,不再需要行为人具有相应的民事行为能力、意思表示真实等传统合同的生效要件,因而也不存在效力待定、无效与可撤销等情形。然而,合同之所以能具有法律约束力,源于法律的赋予。换言之,因为合同当事人的意思表示不违反社会公序良俗,不违反法律强制性规定,因此,在私法视域下,充分尊重当事人的意思自治,并对其给予法律上的充分保护。智能合约的特殊法律构造,使得其绕过了合同生效的要件,一旦成立即已生效。这意味着智能合约架空了合同法中关于合同生效要件的法律约束,使传统的私法法律评价体系形同虚设。^②

2. 保险智能合约成立后合同变更权、合同解除权的丧失。作为私法的合同法,基于双方当事人的合意可以在合同签订后解除、变更合同,并保障当事人的合法权利。《中华人民共和国保险法》(以下简称《保险法》)第 20 条规定投保人与保险人均享有保险合同变更权;《保险法》第 15 条规定投保人享有保险合同的解除权。在保险智能合约中,智能合约一旦发布在区块链中,设定的条件触发后便自动执行,该种模式使得当事人的意志一旦写入代码中,上链后经过区块链验证,条件触发时智能合约自动运行,投保人将丧失保险合同变更权与解除权。智能合约不对交易双方的身份进行区别,只按照编写的代码来执行程序,这种封闭式的运行模式无法将弱者保护理论等价值判断植入合同中,使得保护保险消费者的理念无法在保险智能合约中体现。

3. 保险智能合约单一封闭性导致的漏洞追责问题。智能合约漏洞分为两种情况,一种与传统合同缔约过失责任或违约责任相似,适用过错理论进行追责即可。例如,若智能合约产生漏洞是代码编写人员的疏忽造成,使代码无法执行交易双方约定的内容,则应由代码编写人员承担赔偿责任。另一种情况是代码漏洞。前已述及,智能合约不可避免地会存在代码漏洞,在“以太坊”事件中,“黑客”便是利用智能合约的编码漏洞窃取了区块链货币。在能够获得“黑客”身份信息的情况下,可直接要求“黑客”承担赔偿责任。但是,区块链的匿名性,且智能合约都是在开源的平台订立,“黑客”侵入很难识别,“黑客”的真实身份更是难以查实。^③ 为此,很多正在建设的区块链平台都采用“授权模式”进行商业活动。该种模式是在一个限定的区块链中,一个或多个网络运营商充当“看门人”角色,只允许参与者在被识别并符合适用的访问标准后才能从事交易行为。^④ “授权模式”的优势是使每个进入区块链的身份都确实可查,当出现违法行为时可明确责任主体。但是,“由于在授权的个人、组织或行业的层面上使用区块链,必然导致开放的区块链变成一种内部数据库,当区块链丧失交易主体多元化及交易范围广泛化的特征时,智能合约高效率与低成本的特性也将被打破”。^⑤

(三)“命令—控制型”监管向“去中心化”监管转向

^① 参见王利明、杨立新、王轶、程潇:《民法学》,法律出版社 2017 年第 5 版,第 591 页。

^② 参见王潺、杨辉旭:《智能合约的私法挑战与应对思考》,《云南社会科学》2019 年第 4 期。

^③ See Scott A. McKinney, Rachel Landy, Rachel Wilka, Smart Contracts, Blockchain, and the Next Frontier of Transactional Law, 13 Washington Journal of Law, Technology & Arts, 333 (2018).

^④ See Jenny Cieplak, Simon Leefatt, Smart Contracts: A Smart Way to Automate Performance, 1 Georgetown Law Technology Review, 425 (2017).

^⑤ 夏庆锋:《区块链智能合约的适用主张》,《东方法学》2019 年第 3 期。

传统保险监管模式通常是“命令—控制”型监管,即监管者依靠事先制定的规则来监督保险公司的行为,一旦保险公司突破规则红线,将会受到监管者的制裁。^① 为了实现监管目标,该种监管模式通常采取“一刀切”的方式,以体现公平和正义。而保险智能合约的出现,将颠覆传统的保险监管模式,转向“去中心化”的监管。详言之:

1. 去中心化与中心机构之间的矛盾。区块链技术应用与保险机构的首要困难,是前者分散式运行特点如何与后者集中式管理方式的融合。在保险业中,保险消费者作出正确理性决定的前提是掌握足够且有用的信息。^② 现今的保险产品往往包含复杂且专业性极强的格式条款内容,保险消费者通常无法完全理解其中的含义,且保险合同采取的是格式合同的形式,投保人只有“签与不签”的权利,因此保险消费者是信息不对称的弱势一方。^③ 而去中心化的区块链技术能有效消除保险集中管理方式导致的信息不对称,从而有利于保护保险消费者的权益。与此同时,保险业赖以生存的“大数法则”原理,要求保险机构进行集中管理,这种模式保证了投保人的投保信心以及出险时保险公司进行赔付的能力。然而,分散式的区块链难以实现保险机构的集中管理,而集中管理的保险机构又无法对其他区块进行授权,如何将这两种特点截然相反的模式进行融合,是未来保险监管面临的难题。

2. 区块链保险创新应用新增的法律及合规风险与保险智能合约缺乏监管之间的矛盾。现行金融法规体系对区块链金融的诸多应用尚无明确规定。在保险业中,对于保险智能合约应用的效力问题,我国的法律尚语焉不详。易言之,当前我国保险科技的实践是先于理论发展的,因此,对保险智能合约运用引发的技术弊端,若不能得到有效的法律规制,其未来发展前景将会受到公众质疑。^④ 此外,区块链保险智能合约因其去中心化、数据应用部署管理分散的特点,有可能带来法律责任对象确定困难的新挑战。对那些跨越国家地理边界和司法管辖边界部署的区块链金融应用而言,如果没有权威机构而是由松散的自治组织来控制和管理,法律责任的认定和追责将更加困难。

3. 保险消费者隐私权保护与保险欺诈之间的矛盾。在行为监管方面,如何兼顾保险消费者隐私权保护与防止保险欺诈的需求,需要监管部门精准把握。基于匿名制的区块链技术应用在实践中有效保护保险消费者隐私权的同时又增大了监管部门预防保险欺诈的难度。在传统监管模式下,只要锁定客户,通过管理员就可以由后台直接调取中心系统的数据,进而掌握客户账户下的资金往来等信息。但在区块链技术运用环境下,由于没有中心系统,很难锁定客户的多个匿名账户,除非监管者掌握密钥,或者采用复杂的关联性挖掘算法,否则很难了解交易的真实性与合法性。这就极容易被心怀不轨的投保人以及犯罪分子利用,从而带来保险欺诈的问题。随着区块链技术的发展,保险交易情况基本不可观测,不仅较难及时发现人为故意和软件缺陷导致的错误交易,而且难以甄别保险欺诈等非法行为,与保险监管要求相背离。

① 参见张永亮:《金融监管科技之法制化路径》,《法商研究》2019年第3期。

② See Iain Ramsay, *Consumer Protection: Text and Materials*, Weidenfeld and Nicolson, 1989, pp. 41-42.

③ 参见冯果、袁康:《社会变迁视野下的金融法理论与实践》,北京大学出版社2013年版,第48页。

④ 参见赵大伟:《区块链技术在互联网保险行业的应用探讨》,《金融发展研究》2016年第12期。

四、保险智能合约法律风险防控的逻辑思路

保险智能合约产生于典型的科技创新——“保险+区块链”的运用,保险创新与金融安全之间的动态博弈,使得监管者在面对保险智能合约法律风险防控时,须秉持“不盲从、不排斥”的态度,努力寻求智能合约应用创新与保险防控风险之间的平衡,以推动区块链保险科技监管体系的不断完善。科技治理指的是,“将公共治理的理念和方法运用到科技创新过程当中,注重通过纵向跨层级和横向跨部门跨领域的交流进行治理,强调治理过程中充分协商和治理主体的多元化”。^①为此,下文将以科技治理为逻辑线索,从科技治理所蕴含与延伸出的“技术驱动”“多元协同”以及“一般原则与特殊工具的统一”等层面进行分析。

(一)“技术驱动”是保险智能合约法律风险防控确立的基础

科技发展通常被认为是专家学者、科研人员所应关注的话题,与普通社会公众之间距离甚远。社会公众通常是科技发展的受众,他们因欠缺专业知识而只能被动地接受各项科学技术,而对科技发展的治理,则更多的是交给政府机构或专家学者来完成。然而,随着科学技术的发展,现阶段新兴科技集中于信息技术与生命科技领域,这有别于传统的理工类学科,日益凸显出与每一位社会成员的个人信息与生命安全相挂钩,甚至将对人类社会的价值体系造成深远的影响。在信息技术方面,随着大数据的发展,个人信息泄露、“大数据杀熟”、信息过载与信息茧房等问题层出不穷,人们的个人隐私权保护面临新的挑战。在生命科技方面,基因编辑的出现,使人类可能面临整个基因库的人为改变,来自生命与伦理的拷问亟待回答。而这些关涉人类未来发展的法律、伦理、监管等问题,显然不是单纯的科学技术专家所能够解答的。科学技术虽是中立的,但在复杂的社会环境运用下,会产生各种不可预知的风险。若仅仅依靠专业技术人员对其进行治理,则不仅收效甚微,而且会使治理的目标最终落空。^②总体而言,科学技术的发展带来的是影响巨大的“创新性破坏”,具有很大的不确定性,甚至有可能重新配置社会价值体系,从而对社会效应产生难以估量的影响。为此,如何对科学技术未来发展的走向进行把控并思考其可能造成的后果是十分重要的,但这显然不是科学技术人员所能完成的任务。对这些新兴技术进行的社会治理即科技治理也应运而生。

保险智能合约法律风险防控刚好契合了“技术驱动”的科技治理理念。一方面,伴随信息数字技术发展的保险科技,每天都在生成与处理海量数据,保险智能合约为保险消费者提供个性化定制保险。现代保险业虽然已经发展出针对不同风险的多个具体险种,但对风险发生的环境实际上并没有较为精确的把握,保险公司往往只能运用大数法则,并按照过往综合场景下风险事件发生的概率进行产品设计。区块链技术的运用为保险创新提供支持,保险公司可以约定基于不同场景承担不同的保险责任,风险一旦发生,若满足保险合同中的保险责任承担条件,则可自动理赔。例如,被保险人在自驾游期间突然遇到极端恶劣天气,可以通过临时提高保障程度应对驾驶风险,但天气好转之后即可降低保险保障条件。另一方面,保险智能合约依托区块链技术能提

^① 赵胤:《从科技管理走向科技治理》,《人民论坛》2019年第7期。

^② See Kathrin Braun, Cordula Kropp, Beyond Speaking Truth: Institutional Responses to Uncertainty in Scientific Governance, 35 (6) Science, Technology & Human Values, 771 (2010).

供便捷安全的保险体验。智能合约能够完成理赔处理的自动执行,对客户而言,这是一种可靠且透明的支付机制,而且智能合约能够用来强化具体合约规则。^① 目前我国阳光保险集团股份有限公司推出了业内首款具备区块链特性的微信保险卡单。依托区块链技术,客户可以便捷地进行保险卡单的购买和转赠,保险公司和保险消费者可以追踪保单的流转过程,从而确保产品的真实性和保单的唯一性,杜绝潜在的欺诈风险,也为客户带来更加便捷的保险购买和使用体验。与此同时,保险科技治理者围绕保险智能合约,对各种产品的数据进行收集、存储、分析以便及时发现风险并对其进行规制。

(二)“多元协同”是保险智能合约法律风险控制明晰的方向

科技治理在机制设计上强调“多元协同”,与传统“命令—控制”式监管不同,科技治理从具体的决定和内容中适度抽离,侧重于由谁、按何种形式来作出决定。换言之,多元协同的机制设计为科技治理提供了整体性的流程指引。具而言之:(1)科技治理需要更加完备的知识基础。社会生活正逐渐被各种新科技手段渗透,风险与发展相伴相生。治理者仅仅依靠单纯的科技知识,难以有效化解各项群体的、个人的复杂社会问题,还需更加完备的社会知识来加以辅助。多元协同的机制设计,能够有效地将不同学科、不同领域的专业人士联通起来,通过沟通协商,将复杂的社会问题有针对性地加以解决。(2)科技治理需要更加合理的程序规范。科技创新将影响社会的各个方面,如人工智能技术驱动的自然语言处理工具、无人驾驶汽车等技术的发展已悄然改变了大众生活。长此以往,科技创新必然影响社会公共事务,社会公共事务又关涉大众的公共利益,不能仅仅依托科学界来进行管理,建立多元协同的沟通平台,恰好契合了社会公共事务治理的内在要求,符合治理者在治理程序上的规范目标。在多元协同的治理平台中,存在更加合理、透明的程序规范。各机构、不同个体之间能够针对与自身相关的权利义务进行沟通协调,并进行适当调整,最终达成一个使多方都能较为满意的最优方案。^② (3)科技治理需要更加稳健的效率保证。决策效率不是指决策过程的快慢,而是基于对决策成本和效益综合考量得出的总体性结论。^③ 科技治理的治理者在科技与社会相互融合的复杂情境下,必须有高效的治理决策。而多元协同的平台建设,为决策者获得完备全面的知识、进行高效的治理打下基础。^④

就保险业而言,在多元协同的科技治理语境下,一方面,保险监管者面对一项保险科技创新产品时,首先要确定需要解决的中心问题,明确利益相关者,设定监管者的政策目标。然后召集所有利益相关者共同商议解决方案,从中选出最优方案,并征集利益相关者的反馈意见,随后进一步修改和测试解决方案,继续反馈循环,直到找到最合适的解决方案。在这个过程中,“政府得以退回到决定权的分配和再界定上的程序设计中,促使被监管的社会经济关系实现‘受规制的自治’”。^⑤ 另一方面,科技治理的多元协同还强调治理者与被治理者之间的数据共享,体现在保险行业中,即为由过去的将保险机构向监管机构的单向数据传输转变为双向数据整合,使得保险监管

^① 参见朱进元、刘勇、魏丽:《保险科技》,中信出版集团股份有限公司2018年版,第193页。

^② 参见[瑞典]英瓦尔·卡尔松、[圭]什里达特·兰法尔主编:《天涯成比邻——全球治理委员会的报告》,赵仲强、李正凌译,中国对外翻译出版公司1995年版,第2页。

^③ 参见卢阳旭:《科技治理就是要让科技创新更好承担社会责任》,《科技日报》2019年11月18日。

^④ See David H. Guston, Building the Capacity for Public Engagement with Science in the United States, 23(1) Public Understanding of Science, 53 (2014).

^⑤ 许可:《从监管科技迈向治理科技——互联网金融监管的新范式》,《探索与争鸣》2018年第10期。

者与保险机构都能共享数据信息,共同参与科技治理。

(三)“一般原则与特殊工具的统一”是保险智能合约法律风险防控理念的突破

科技治理还应强调一般原则与特殊工具的统一。详言之,一方面是有有效的治理需要社会有基本的理念共识和行为规则。科技治理应遵循一些基本思想,达到治理目的,实现公平正义。科技治理面对的是复杂的社会关系、深刻的利益冲突、不同的价值观念以及差异化的行动主体等一系列问题。必须建立一套具有明确标准、大家共同遵守的行为规则,从而达成理念共识,形成被多方主体认可的一般原则。科技治理的出发点与目标是建构与法律规则功能相一致的技术性标准。“标准的规范性是基于制定主体之间的协商一致性,在适用中具有公私兼容特点,既可以通过标准化实现一致性,也可以通过标准化保持差异性,从而符合‘多中心’或‘淡中心化’的治理思路。”^①因此,保险科技的行业机构可以推动技术标准的制定,将其作为合规的基本要求,并借助外部第三方认证机构将其技术标准具体落实,通过监管机构颁布的监管法规加以认可,确保其权威性与可执行性,即“标准—认证—认可”模式。这一模式已付诸实践,《欧盟一般数据保护条例》中的个人数据跨境认证制度、《中华人民共和国网络安全法》第11条对网络安全行为规范这一行业标准的授权均体现出该种治理思路。另一方面,科技治理需要不断更新治理方式,创造适用于新科技场景的治理特殊工具箱。随着科技发展,静态式、人工式的传统监管模式已然应对乏力,亟待监管创新。随着科学技术的持续发展,如果治理无法与时俱进,必然出现治理乱象。为此,只有革新治理手段,开发有针对性的治理工具,才能有效化解各种新问题,实现有效治理。当前,保险科技治理工具的开发可以重点围绕以下几个方面展开:(1)有利于保险创新收益和风险识别的技术规范工具,如建立数据安全与信息保护机制等。(2)有利于多元参与、协同共治的共识形成的倡导工具。包括监管机构与企业、技术提供者等合力推动以实现技术治理、建构数据平台共享机制等。(3)有利于实施法律、政策和社会干预的监管工具,如建立实验性监管机制,监管机构允许适格的保险科技创新企业在特定期间、特定环境中进行保险新产品或新服务的测试实验等。

五、保险智能合约法律风险防控的具体路径

保险智能合约具有提高商业效率、提升服务质量、促进透明度等特征,在给保险消费者带来便利的同时,也可能诱发各类风险,而现有的法律规定在面对保险科技所带来的风险时已捉襟见肘。为此,笔者将在上述保险智能合约的法律构造与法律风险分析的基础上,通过科技治理的法治化模式架构,以“技术规范—机制设计—智能监管”为核心,以防范法律风险为目的,寻求智能合约应用创新与金融安全之间的平衡,以推动区块链保险监管体系的不断完善。

(一)构建保险智能合约法律风险防控的技术规范体系

德国学者萨维尼有言,体系是“法律内在一致性的前提”。^②由此可以认为,构建保险智能合约法律风险防控的技术规范体系,是保险科技监管内在一致性的前提。如果未能构建保险智能合约法律风险防控的技术规范体系,就很难准确、合理地防范保险智能合约所带来的风险。

保险智能合约是内嵌于区块链技术中的代码合同。代码瑕疵、代码漏洞的存在,均表明包含

^① 许可:《从监管科技迈向治理科技——互联网金融监管的新范式》,《探索与争鸣》2018年第10期。

^② 转引自[德]维尔纳·弗卢梅:《法律行为论》,迟颖译,法律出版社2013年版,第346页。

代码在内的技术是风险防控的关键。“技术的参与令风险更加分散,更具有系统性和传染性,会出现监管空白和监管套利,对金融监管和宏观经济带来新的挑战。”^①为此,技术标准的统一与兼容是保险智能合约法律风险防控的前提。详言之:

1. 在保险智能合约技术运行风险管控方面,应基于分级分类原则,明确构建区块链节点间的网络通信安全要求(专线连接、地址绑定、多运营商冗余、通信加密、网络攻击感知及防护等)、应用安全要求(应用安全可控加密算法、密钥管理、数据脱敏保护、节点身份认证、节点权限管理等)和物理安装要求(联盟链、私有链节点布局、数据中心管理、物理设备管理等)^②。既要对接高安全等级的保险业务提出更高的安全标准,以更好地防范“黑客”攻击、信息窃取及安全生产风险;同时也要根据区块链技术物理分散部署的特点,有针对性地调整传统中心化信息系统运行的风险管控标准。

2. 在保险智能合约的“技术—法律”兼容性方面,应规范区块链保险行业应用的参考技术架构与功能视图。在保持功能组件模块灵活可配置的同时,基于效率、资源开销和容错等指标,明确不同类型的共识机制及算法在不同规模区块链实施场景中的适用性;确定区块链数据存储结构标准;确定区块链节点通信消息报文标准;确定智能合约语法、语义和语用标准;确定应用程序访问接口标准,以提升区块链技术应用的兼容性。智能合约特殊的法律构造使得其绕过了合同生效要件问题,可在保险智能合约成立后,由具备法律背景的专业人士审查确认合同符合生效要件后,再将其编为代码发布在区块链中,至于不具备计算机专业知识的表意人通过第三人编撰代码而产生的意思表示错误和风险承担问题,则完全可适用传统的违约与侵权责任。在投保人合同变更权、解除权丧失问题上,可采用混合协议的模式,即将保险智能合约用传统法律语言撰写,同时将其纳入代码,要求区块链和法院一起执行,该代码为法院执行留下编写空间。这种智能法律合约就是数字和自然语言的混合。^③在混合协议模式下,投保人如果有解除保险合同的意愿,经过法院认定后可触发代码执行。在保险智能合约漏洞产生的追责问题方面,较为妥当的一种方式采取“用户信息最低标准”,即通常不对使用区块链的用户信息作录入要求,以保持区块链的匿名性。但若使用的用户出现异常状态或交易信用变得低于基准要求时,才须提供更详细的用户信息。

3. 在保险智能合约技术应用场景适应性方面,应建立不同保险业务场景下区块链技术应用的指导标准和可用性测评规范,并建立该场景下智能合约条款的审计标准,引导市场根据应用场景特点,有针对性地应用区块链技术,防止盲目跟风。例如,现阶段接受保险智能合约的用户,通常是年轻的保险消费者。他们更易于接受新生事物,不惧在精益和敏捷方式下快速发展的保险创新产品。在保险智能合约日常的管理实践和运营中,面对年轻的保险消费者,应嵌入先进的、符合年轻人投保习惯、投保心理以及投保偏好的分析方法,从而有针对性地作出监管决策。

(二)建立保险智能合约法律风险防控的多元协调机制

^① 张永亮:《金融监管科技之法制化路径》,《法商研究》2019年第3期。

^② 参见杜宁、王志峰、沈筱彦等:《监管科技:人工智能与区块链应用之大道》,中国金融出版社2018年版,第184页。

^③ See Primavera De Filippi, Aaron Wright, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018, pp.76—78.

保险智能合约法律风险防控的有效应用需建立多元协同的协调机制。这种机制应包含保险机构、保险消费者、技术提供方、监管方等多方利益主体,从产品设计开发、数据规范应用、智能理赔服务等多方面进行沟通协商,寻求彼此间效率最大化的最优路径。多元协同机制旨在通过不同主体之间的对话交流,改变过去监管者单一决策的方式,建立沟通不同主体之间的沟通桥梁,通过这座桥梁,各方利益主体能够充分地提出自身诉求,并在治理过程中得到落实。^①然而,现阶段我国缺乏各方主体之间展开对话的平台,未能建立多元协作、共同协商的机制。具体而言,保险科技法律风险防控还缺乏监管者、技术提供者、保险公司、保险消费者之间的交流与合作。在多元协调机制中,监管者具有问题导向意识,技术提供者具有专业技术,保险公司具备产品导向与市场导向的特色,保险消费者可从客户视角与用户需求方面提供治理建议。通过建立多元协同参与的协调机制,增加对话交流,形成优势互补。

在保险业中,许多保险机构缺乏完整的数据库,在数据分析上存在片面性,而保险监管者虽然有较全面的数据信息,但是在监管方式、手段方面,往往滞后于保险创新,监管效率不高。技术供应商徒有技术,却无法与保险公司、保险监管者进行良好的互动。有鉴于此,建立一个多方参与、共同合作的协调机制,使得监管者、技术提供者、保险机构与保险消费者围绕共同解决方案进行沟通对话,为保险科技监管产品在开发阶段制定明确的技术标准,各方主体分工协作,技术提供者在软件开发上具有专业视角,保险机构在保险产品设计上兼顾市场需求,保险消费者从用户体验方面提供建议,并由立法者提出保险科技产品的明确监管指标与触底红线标准,对促进保险智能合约的监管将具有重大促进作用。长远来看也将对保险科技创新整体产生深远影响,有利于保险科技的高效应用。

(三)创设保险智能合约法律风险防控的智能化监管制度

智能化监管是保险科技发展背景下的一种全新监管模式,是具备多样性、数字化、自动化、法制化的特殊监管工具。具体而言,包括但不限于以下几个方面:

1. 强化区块链保险应用的准入管理。技术上的去中心化并不等于监管上的完全去中心化,更不能等于法律责任的分散化。监管部门应强化区块链保险应用的准入管理,加强区块链保险服务提供者的事先审核及账户册备案,限制以开源社区、行业联盟等名义依托区块链开展保险业务的行为,明确只有具备保险业务资质的法人单位才能发起相应保险智能合约的应用,并承担相应的合规责任。

2. 明确在区块链保险应用中需由监管部门控制监管节点的总体原则与实施方式,以确保监管部门能够在非中心化区块链中有效地履行监管职能。应基于穿透式监管理念,^②在允许业务参与方身份“前台”(区块链节点)匿名保护的前提下,视业务类型向“后台”(监管节点)公开参与方的实名身份。区块链保险机构主体应向监管节点提供可视化的监管工具,以便监管部门实时掌握系统的技术及应用运行整体情况,定制化地完成监管统计分析工作。

3. 建立实验性监管机制。实验性监管机制是指监管机构允许适格的金融科技创新企业在特定期间、特定环境中进行金融新产品或新服务的测试实验。换言之,即监管者创造一个安全空

^① See Francesca Musiani, Practice, Plurality, Performativity, and Plumbing: Internet Governance Research Meets Science and Technology Studies, 40(2) Science Technology & Human Values, 272 (2015).

^② 参见荀文均:《穿透式监管与资产管理》,《中国金融》2017年第8期。

间,使金融科技创新企业可测试其创新的产品、服务、商业模式等各个方面的可行性,而又不需要承担一般违反金融监管法规的责任。保险区块链监管之所以需要实验性监管模式,是因为一方面保险智能合约的本质是科技创新者为传统保险服务业带来的竞争与创新,故在监管法规的设计上,需强化保险消费者对新科技的信心,使消费者愿意购买保险科技的创新商品或服务;另一方面,监管法规若设置过高的门槛,将阻碍保险科技创新者进入保险市场,反而不利于竞争与创新,建立实验性监管机制,使保险科技企业在宽松的监管法规环境中探索,方可实现促进竞争与创新之目标。在实验性监管模式下,通过豁免其遵守相关监管法规义务的方式,使被监管者的测试产品在测试期间取得相关的实证经验,并进行调整,以促进其成长并发展完善。这种模式的主要目的是加强监管当局与金融科技创新企业的沟通交流,提早介入,由传统的“先发展后监管”变为“边发展边监管”,全程了解金融科技的进展情况及相关信息并进行政策辅导,从而使监管者与被监管者之间建立可信赖、持续性的良性监管互动,提高监管部门的监管效率。^①

4. 完善保险智能合约法律条款与区块链保险行业法规。在完善保险智能合约法律条款方面,应在现行电子证据司法认定标准的基础上,明确区块链记录作为数字化资产权属存证及流通的法律效力、保险智能合约作为电子合同的法律效力和争议发生后的证据证明形式(记录智能合约如何作为呈堂证供等)、裁决执行方式(裁决结果如何在区块链记录中更新体现)以及诉讼司法管辖权确定方式(匿名性和分布式记账技术特点下如何确定司法管辖地域与冲突规范下的准据法)。在完善区块链保险行业法规方面,应基于功能监管和行为监管原则,在审视原有同质业务法规条件、解决原有条文与区块链技术的适用协调性问题的基础上,进一步对每一类共性区块链保险应用场景明确统一的监管原则,不留监管死角。紧密跟踪区块链保险业态的变化,及时设立负面清单,明确不得依托区块链技术开展的保险业务类型。对不在负面清单中的保险业务类型,也应及时根据业务特点,分别相应地明确统一的业务标准、监管制度和保险消费者保护指南,给予保险市场明确的预期。

5. 加强技术设计人员资质认定与考核体系建设。区块链技术不是绝对安全的,毕竟区块链各节点的设计是由人完成的,这可能产生难以发现的技术漏洞。监管部门未来应规定技术设计人员应该经过考核并获得相应资质后才可上岗;应设立动态资质认定考核体系指标,持证上岗的技术设计人员须定期重新考核认证。此外,监管部门还应加强对公众关注度高、制度约束不严、炒概念或保险欺诈风险迹象明显的区块链保险业态的整治,避免局部风险扩散影响整个保险市场乃至金融秩序的稳定。

六、结 语

近年来,在以数字化、网络化、智能化为特征的信息化潮流推动下,保险科技通过保险与科技的深度融合发展,在保险领域表现出新的实现方式、服务形态、业务模式,迅速成为一个备受全球瞩目的热点议题。在我国,“金融科技应用的广度、深度和精度不断增强,提升了金融服务质量和效率,惠及了广大金融消费者,在不少领域形成了独特市场优势和规模优势,为服务实体经济、防

^① 参见许多奇:《互联网金融风险的社会特性与监管创新》,《法学研究》2018年第5期。

控金融风险、促进金融改革和开放提供了重要驱动力”。^①与此同时,随着保险科技的发展,保险创新产品层出不穷,在增强保险分散风险能力、提高保险服务水平、为保险消费者提供更多便利的同时,也对现行的保险监管提出了巨大挑战。保险科技法制是否完善,不仅是衡量一个国家保险法制是否健全的重要标准,也是判断一个国家经济体系和治理能力是否现代化的重要标志;保险科技之制度设计与立法完善,应服务于我国数字经济时代发展之具体需求,与时俱进。笔者在此所探讨的保险智能合约是“保险+区块链”运用的体现,区块链虽然是去中心化的、放权的技术,但是其并非完全取代原有的中心化机构,而是促进各领域的多中心化机构达成联盟,由“从上至下的强制性”向“从上至下的协商性”转变。同时,作为“技术驱动”的监管科技,其使命不仅在于对主动的、动态的、分布式的保险智能合约法律风险防控目标的追求,更在于为强化我国保险科技监管、增强保险监管的专业性和穿透性提供法治框架。

Abstract: Insurance smart contract is the construction method of “code is law”, that is expressed as code when the contract is established; the contract is effectively expressed as blockchain verification; and the contract execution is expressed as automatic software execution. Insurance smart contracts can realize the automation of claims processing, reduce human intervention, shorten claims time, and have wide application prospects in the future. At the same time, insurance smart contracts as code contracts may have code loopholes and code flaws; they have a single closed nature; and legal risks such as conflicts between “decentralized” supervision and traditional supervision concepts. Therefore, under the development trend of the combination of smart contracts and insurance, taking scientific and technological governance as a logical clue, from the three levels of “technological drive”, “multiple coordination” and “unification of general principles and special tools” contained in scientific and technological governance, design the basic framework of insurance smart contract legal risk prevention, and then propose a specific legal path of “technical specifications—mechanism design—intelligent regulation”.

Key Words: blockchain, insurance smart contract, legal structure, legal risks, science and technology governance

责任编辑 翟中鞠

^① 孙天琦等:《金融秩序与行为监管——构建金融业行为监管与消费者保护体系》,中国金融出版社2019年版,第131页。