

合同自动化的等级序列、展开维度与风险防治^{*}

唐子晗

(中南财经政法大学 法学院, 湖北 武汉 430073)

摘要: 从合同自动化的等级序列入手, 通过类比自动驾驶对合同自动化的差异化发展问题进行探讨, 指出智能法律合约想要转换为智能合约需满足文法要求、平台访问、非赋权原则三个基本规则。结合合同生命周期对智能法律合约的运行过程进行系统化的展开, 进而对不同阶段的智能法律合同所聚焦的问题进行论证。通过分析智能合约自动执行与法律合同中当事人享有权利之间存在的内生矛盾引出智能合约的风险原点, 并加以讨论和评价。最后, 摆脱代码之治这种单一化的风险救济途径, 通过构建覆盖事前、事中、事后全流程的智能合约风险闭环机制, 为探索智能合约可持续发展提供新的可行性方案。

关键词: 合同自动化; 智能法律合约; 智能合约; 人工智能; 风险闭环

中图分类号: D922

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2023.11.012

引用格式: 唐子晗. 合同自动化的等级序列、展开维度与风险防治 [J]. 网络安全与数据治理, 2023, 42(11): 64-71.

The hierarchical sequence, unfolding dimensions, and risk prevention of contract automation

Tang Zihan

(Law School, Zhongnan University of Economics and Law, Wuhan 430073, China)

Abstract: Starting from the hierarchical sequence of contract automation, this paper explores the differential development of contract automation through analogy with autonomous driving, and points out that in order to convert smart legal contracts into smart contracts, three basic rules must be met: grammar requirements, platform access, and non empowerment principles. Systematically expand the operation process of smart legal contracts based on the contract lifecycle, and then demonstrate the issues focused on in different stages of smart legal contracts. By analyzing the inherent contradiction between the automatic execution of smart contracts and the rights enjoyed by parties in legal contracts, the risk origin of smart contracts is derived, and discussed and evaluated. Finally, by breaking away from the single risk relief approach of code governance and constructing a smart contract risk closed-loop mechanism that covers the entire process before, during, and after the event, a new feasible solution is provided for exploring the sustainable development of smart contracts.

Key words: contract automation; smart legal contracts; smart contracts; artificial intelligence; risk closed-loop

1 合同自动化 vs 自动驾驶: 等级序列下的差异化发展

伴随着数字化的发展, 与数字流程相脱节的静态合同正在逐步退出历史舞台, 取而代之的智能法律合约正在迅速改变合同的运行模式。随之引发的关于如何在保证商事合同充分享受自动化红利的同时, 保持合同的法律完整性和可执行性的世纪难题成为了法律科技进一步发展必须面临的挑战。当前, 法律行业在法律程序和法

律文书的形式和功能等方面都正在进行数字化转型, 例如使用软件自动创建合同模板和由人工智能支持的大规模文件审查。这种融合的趋势也促使律师们一直在努力寻找如何在商业关系中利用自动化重构合同的运行模式, 同时又能保持合同的法律约束力和可执行性的可行方案。对此, Blycha & Garside 提出了智能法律合约 (Smart Legal Contracts, SLC), 即一种包含一个或多个自执行组件来减少或消除合同过程中人工干预的因素, 并且可以由机器 (部分或全部) 创建、执行、管理和维护的法律协议^[1]。

^{*} 基金项目: 国家重点研发项目 (2022YFC3340900)

智能法律合约是在传统现实合约基础上进行形式化提取、着重于合约程序性和法律性共举的合约形式，可以通过转译机制转化成智能合约，从而进行程序运行，其目的在于在现行法下将智能合约形式及其代码执行行为认定为法律意义上的电子合同^[2]。并且，从理论上讲，智能法律合约是对传统现实合约的形式化、模板化表达形式，属于法律合约且可转化为智能合约。但是能否转化成功很大程度上取决于合同自动化的水平高低。基于此，可以在合同自动化水平和自动驾驶汽车执行动态驾驶任务的自动化水平之间做类比，根据合同自动化的水平高低对其进行分类（如表1所示），从第0级（无自动化和无自动化合同绩效）到第5级（完全自动化和全自动合同绩效）^[3]。其

中，每一个级别的细微差别都代表了合同性质与操作方式的转变，特别是从第3级到第4级的转变中，合同自动化运行将面对合同条款和数字托管平台授权的条款之间相互作用的问题。随着传统合同向智能法律合约发展，合同也从单纯对权利与义务的静态记录逐渐演变为兼具促使、审计以及记录合同绩效的“智能生命体”。这种转变一方面意味着合同的形式和功能开始依赖于数字技术的不断驱动，其自身也在逐渐向更加完整意义层面的机制设计迈进。另一方面，合同创建的自动化不同于合同履行的自动化，两者面向的是不同的法律问题。本文旨在为律师澄清合同自动化内部的发展关系，并进一步探索在第3级到第5级中智能合约的运行逻辑与风险防控。

表1 合同自动化分级示意图

	传统合约			智能法律合约		
	级别0	级别1	级别2	级别3	级别4	级别5
合同特性	文本无法通过数字方式访问	文本可以通过数字方式访问，但不能由计算机进行语义处理	数字可访问和部分文本可以由计算机语义读取和处理。每个不分都有一个单独的、数字可访问的版本	数字可访问和存储在一个专门的数字平台上，提供一个同步的“只读”共享视图	除了与第3级相同的以外，第4级再加上共享的“读写”访问合同，并自动履行合同约定指定的、约定的行为（法律生效后签署）	除了与第4级相同的以外，没有任何人工干预（法律生效后签署）
人员参与合同履行的程度（法律执行后）	人员通过使用软件系统，需要手动监控和履行合同约定下的义务和行使权利			人类交易对手使用合同的共享数字实例（法律签署后）来监控和履行合同权利和义务	机器在商定的参数范围内监控和执行自动的合同行动。与外部来源的互动以及双方作出的选择都不可改变地记录在合同中 在预先商定的情况下，可能需要人工确认或选择特定的性能	监控或执行不需要任何人的行为。合同行动已“被执行”
具体功能	以书面形式提供合同证据的静态记录。扫描副本的结果是数字版本，可以通过数字共享、存储和复制，但仍然不能被除页面图像以外的任何级别的计算机处理	提供合同证据的数字记录，可以轻松通过计算机搜索和分析，以及共享、存储、打印和复制	与第1级相同，某些合同数据由内部系统的机器可读性（通过手动或自动化方式）进行分类。这些数据可以与该部分的数字系统集成，无需人工干预即可进行处理。然而，与第4级不同的是，这一处理是由单一的一方进行的，并不影响合同的权利和义务（因为每一方的单独的合同记录仍然是只读的）。可以在创建阶段通过文档自动化过程来识别和创建结构化的数据	合同的数字实例托管在一个相互可访问的平台上（例如一个分布式账本技术平台）。该合同的数字实例是在交易对手方之间商定的，作为该合同证据的一个真实记录，以数字形式存在，是一种共享的数字资产。双方对共享记录有“只读”的访问权限，这些共享记录可以集成到双方的内部数字系统和过程中	与第3级相同，以及合同部分性能的自动化与外部系统和数据源的集成。双方和外部数据源可以以“读写”的方式与合同进行交互，以合同形成/法律执行时预先约定的方式记录合同的履行情况并改变合同的状态。将共享的、最新的数字资产与内部业务系统（如ERP软件）进行集成。为数据分析提供数据生成和捕获。唯一的真相来源。对合同履行产生的数据进行审计跟踪	与第4级相同，但所有合同履行都是完全自动化的，在特定的、合适的用例中无需人工干预

2 展开维度: 跨越合同生命周期的智能法律合约

伴随着区块链与人工智能等技术在合同生命周期的不同阶段的深入应用, 这些技术在周期中的功能也逐渐明确。比如人工智能对合同起草、审查都是效率层面的提高, 但是其并不会内在地改变合同本身的功能。然而, 智能合约的出现则是促使智能法律合约能够自动履行合同义务, 并逐步改变了合同的固有功能, 使其更多地作为双方签订合同的证据, 而不具有法律层面的约束力。由此可见, 在合同生命周期的不同阶段, 智能法律合约具有不同的表现形式、功能与法律效果^[4]。

首先, 由于需要充分了解项目的性质与要求, 因此合同订立始终都是法律实践中一项具有挑战性的任务。因此许多的合同起草技术公司已经开始试验利用机器学习算法实现合同起草的自动化, 并且其均需要获取大型数据库中的合同来训练算法。然而, 由于合同生成工具仅限于预加载的合同语言, 因此无法满足特殊客户或者交易类型的需求。因此, 一些法律从业者批判合同生成工具只能提供“填补空白”的功能, 不能生成定制类合同。并且, 合同履行数据的匮乏以及各方在公共数据库中公布合同语言和履约信息的现实障碍都为合同起草自动化的发展蒙上了一层阴影。为了解决上述问题, Nick Szabo 提出可以通过运用完善的合同管理系统对每一个合同进行跟踪、审查与评估, 由此产生可靠的合同绩效数据。这些绩效数据可以阐明相应的合同条款的价值, 进而以帮助机器学习过程筛选“垃圾数据”, 提高算法的准确度。另外, 合同生成工具的机器学习往往需要获得有价值的私人合同。然而, 在实践中律师事务所可能不愿意分享他们花费时间生产的合同语言。因此, 一个潜在的补救办法就是加强对创新性合同语言的知识产权保护。通过对具有创新型的合同语言予以商业秘密的保护, 可以鼓励律师们分享他们所产生的有价值的合同语言。反过来, 律师们也可能会进一步投资开发创新的计算机处理语言, 增加和提高合同数据的数量和质量, 为市场增加更多的价值。

其次, 大多数律师承担的一项常规但复杂的任务就是合同解释, 律师往往需要从合同中的措辞中推断出客观意图, 从而回答有关当事人达成协议的特定问题。其中, 合同解释的第一步就是明确当事人之间有争议的问题, 该问题可能涉及合同的任何事项, 比如股权出售中的附条件条款的性质等。第二步就是提出有争议性问题的潜在答案。合同解释的第三阶段则是最为耗时的阶段, 它包括了审查法院认可的司法解释, 从而确定支持每种解释论点的相关因素, 这些相关因素包括了整个法律文

本, 词语的潜在含义、背景以及合同目的、每种解释的潜在后果和商业常识等标准。事实上, 基于人工智能技术的法律问答系统 (LQA) 可以在一定程度上解决合同的解释问题。然而, 合同解释自动化需要机器学习具有推理能力和文本理解能力, 即需要机器一方面搜索并理解合同中单词的潜在含义, 另一方面则是确定哪一种潜在含义更符合合同的真实意思。有学者指出可以构建分类—预测性或分类输出的合同解释模型, 该模型可以通过分析相关类别的合同数据集来训练自身, 以便识别特定条款。该模型的目的是根据输入数据是否构成特定类型的解释论证的基础对输入数据进行分类, 其中包括了语言、文本、目的、结果或规范等。由此同时, 在机器学习可以识别并分类解释性争议的前提下, 那么就需要相应的自动化机制来解决争议。由于解释性争议往往是通过权衡相互对立的观点来确定的, 从而得出双方最有可能的真实意思表示。其中, 机器学习可以基于四类参数构造合同权衡机制: (1) 确定正在考虑的选项; (2) 确定支持每项选择的因素; (3) 对每个选项进行评估 (即确定“每个选项相对于其他选项的偏好强度”); (4) 确定在结合不同因素的评估时对每个因素的相对重要性。然而, 有的学者也指出预先权衡这些因素的范围也是极其有限的, 并且这种每个论点的数字分数也几乎完全取决于人类的判断, 没有形成突破性的技术进步。基于此, 不妨构建一个模型来预测解释性纠纷的结果。在这种模型中, 机器根据数据进行自我训练, 以便在给定输入因子的情况下可以以预测的形式产生输出, 从而将其应用于识别权衡成功的参数模式。

再次, 随着自然语言处理 (NLP) 技术的最新进展, 为了提高法律从业者的审查效率, 实务界开始认识到机器学习模型可以学习自动提取和识别合同中的关键条款。到目前为止, 市场上已经有大量的法律科技公司开发和提供自动化的合同审查工具。2021 年 5 月 Atticus 项目公布了合同审查的 Atticus 数据集 (CUAD), 这是一个专门用于法律合约审查的新数据集。该数据库由数十名法律专家创建而成, 其中包括了超过了 13 000 个注释, 可以实现从合同中自动提取和识别关键条款^[5]。与之相对的, 近日 BlackBoiler 通过创建新的仪表板和剧本创建选项来彻底消除训练数据的烦恼。用户可以直接在 BlackBoiler 平台上快速构建谈判手册, 以使用新的剧本构建器功能为其自动合同标记提供支持。BlackBoiler 将从用户的法律剧本和历史合同中学习, 然后将关键条款与首选合同条款的剧本进行比较, 并识别不合规的合同语言, 然后再为特定条款和整个协议分配风险评分。

最后,智能合约作为一种自动执行合同条款的计算机代码,其可以在不依赖合同双方手动操作以及法院的调解的情况下自动化执行双方的承诺,如图1所示。对于智能合约而言,代码由计算机执行,法律合约(文本合同)决定了法律关系。在传统合同中,法律文本与法律关系有着内在的联系。然而,对于智能合约而言,代码(智能合约)和法律合约(文本合同或默示合同)之间没有内在的联系。计算机并不关心人类将如何理解这些代码,因此法律解释对于智能合约而言也是不可能实现的。但是,智能合约又通常需要面对现实世界的未知变动,因此仍需要将人工执行链的一部分重新引入到智能合约的自动执行链中,即让合同双方可以控制合同的执行^[6]。

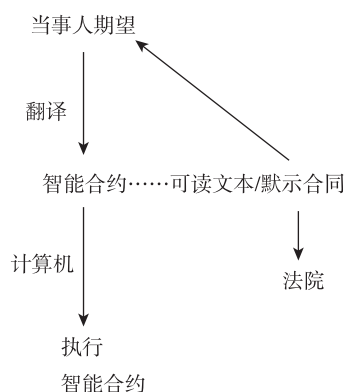


图1 智能合约生成过程

例如,为了能够应对例如像建筑施工合同这类涉及主体众多,协调利益较为困难的合同类型,能够确保缔约双方自愿遵守其在合同签订之日所记录的自己的意愿,并约束其行为,在实践中,建筑施工智能合约将从公共数据环境(CDE)接收数据,只要满足了所需的条件(根据CDE中相关各方共享的数据),合同义务将在几秒钟内自动执行,而无需人工干预。进一步的研究应该努力确定不可抗力等原则如何得到充分实施。另外,为了能够使得不可抗力在合同领域有着更加广泛的生存空间,Ratna Januarita 和 Yeti Sumiyati 则是基于风险管理框架创造性地提出了新冠肺炎疫情背景下合同中LRM的框架设计^[7]。基于风险管理框架,从合同签订前到合同结束,合同相对方在缓解COVID-19影响的前提下,达成了对有关不可抗力的导向协议,因此形成长期的业务关系。并且,风险管理架构也可以充当第三方数据集,LRM模型中的这些数据(信息)通过一个相互访问的在线空间共享,可用于改善合同相关方之间的知识转移,进而保证不可抗力的认识协调问题。数据(信息)可实

时提供给合同相关方,从而减少了信息的不对称性,并防止了由于信息的不完整或延迟获得而导致的分歧和争议,而智能合约也可以发挥其自动执行的功能,实现不可抗力条款的自动执行。最后,LRM模型可以被视为支持合同项下的索赔和争议的有效工具,其可以通过提供可靠的当代记录,同时创建、获得或产生的索赔或争议所基于的事实,协助合同相关方更好地完成举证责任。

3 智能合约风险闭环的管理设计与防治路径

事实上,基于区块链的智能合约只是接管了传统合约的执行功能,但是并没有“继承”合同解释的作用。由于智能合约依赖于自动化的执行链条,因此缺乏对合同执行过程中显失公平的纠正程序,合同当事人必须信任智能合约的提供平台,而不是他们的交易对手。同时,如果智能合约的开发者故意或者过失没有正确执行双方的法律规则,由此造成的损失现阶段却也无法有效地援引法院监督。因此,为了能够完善合同自动化中智能合约的运营,则需要从事前、事中、事后三个方面对其加以规范,进而构建智能合约的风控机制。

3.1 风险起点:合同自动化的不灵活性

智能合约的不灵活性体现在合同生命周期的某些或所有阶段(从搜索和起草到履行和执行)。对此,有的研究者提出了“法律代码化”的主张,主张使用编程语言将法律转化为代码,并写入智能合约形成参数,促使不符合参数规定的履行条款无法被正常执行。这种将法律条文事先嵌入智能合约文本的办法虽然可以确保自动履行出现问题时,智能合约可以依据转化为代码后的法律自行解决问题^[8],但是诸如合同法中的“善意”或者“忠诚勤勉”等义务却难以转化为计算机代码。法律规则的模糊性与算法规则的准确性之间具有天然的矛盾,法律纠纷的解决依赖于责任规则与赔偿规则的适用,这些规则都具有很强的灵活性,需要法官针对具体案情作出具体判断。这也就意味责任规则与赔偿规则很难转化为智能合约代码。由此可见,通过代码重新定义法律规则,建立智能合约条款的语言审查机制,从而逐渐实现法律规则转化为代码的想法,现阶段只能被视为一种发展方向,但实际操作起来仍存在较大的困难^[9]。

并且,还有的软件开发人员正在区块链上添加“许可”命令,以方便在智能合约履行过程中进行人为干预。有的开发人员还在尝试开发私有区块链与混合区块链,通过区分可以被介入的智能合约与不能被介入的智能合

约以解决上述问题。其中,第一种方案就是建立公开可用的受管控的数据库,缔约方可以将其输入到智能合约中,以便随时了解不断发展的法律规则;第二种是通过当事人或者其他代理人承担更新代码的责任,并对当事人进行事后审查。尽管这两种解决方案似乎都具有可实施性,但是数据库本身却会很大概率地提供错误的数据(信息),在这种情况下,双方将面临谁承担这种缺陷风险的问题。另外,由于审查代码需要花费时间、精力与人力,因此智能合约的事后审查也将导致依赖智能合约的效率理由逐渐开始受到侵蚀。尽管伴随着 ChatGPT 的推出,有的学者也指出 ChatGPT 作为一种在大量数据上训练的语言模型,可以帮助智能合约实时分析和解释法律数据,从而实现更准确、更高效的跟踪和管理^[10],然而,必须要承认的是智能合约代码仍然缺乏某些必要的人类素质,即机器无法培养同理心、公平或正义感,这也说明了与商业环境隔离的机器学习并没有达到理解和执行自然语言的阶段,并且其可以像法官那样通过知识和经验来解释合同各方的特定意图^[11]。随之而来的是,Paech 提倡将智能合约与人工合同进行组合。这种解决方案允许当事人修改协议的某些部分,并处理不可预测的情形所产生的影响。但是这种将人工合同与智能合约的组合方式却也会导致成本增加,最终这种解决方案势必会抑制缔约方使用智能合约的积极性^[12]。与此同时,合同自动化的不灵活性也造成了实践中纠纷频出。例如,在 Quoine 有限公司诉 B2C2 案中,新加坡国际商事法庭及上诉法庭认为在 Quoine 向 B2C2 开放 API 接口接收其卖盘报价和 ETH 买方被系统强制平仓买盘这样的程序化自动交易过程中,买卖双方客观上都没有机会实际意识到另一方可能发生的认识错误并加以利用。通过回溯 B2C2 设定深度价格的技术和交易背景,也无法得出其有利用交易对手价格认识错误的目的。所以不存在普通法下的单方、双方或共同错误。Quoine 不得据此主张合同无效而回滚交易。

3.2 基于 Oracle 网络的代理智能合约

为了执行和处理智能合约,区块链经常需要融合各种来源于真实世界数据集成或依赖使用第三方服务。尽管区块链本身是一个安全的生态系统,但是恶意操作者操纵外部来源的数据仍然使其面临着安全风险。与此同时,为了帮助防止由于编码错误或测试不充分的智能合约而导致的大规模不一致的情况发生,需要从技术层面改良智能合约的运行模式,即需要一个完整的事前操作规范,以此确认合同双方的共同期望是否被正确性地编入合同^[13]。

在实践中,DON 系统是区块链和各种现实世界数据

源之间进行沟通的中介系统,其中最具有代表性就是 Oracle 创建的一个甲骨文节点的网络模型。在该模型中,区块链可以从多个来源安全地从经过身份验证的数据源中获取数据,并由相关方进行交叉核对。与此同时,该模型(如图2所示)通过确保信息冗余来防止整理信息时出现的单点故障,启用混合智能合约,以便链外数据/事件可以触发链上合约的执行。例如,ChainLink 为了能够建立安全通道,通过链上代码安全地传输和消费外部信息和服务,便提供了高水平实用性以及易于开发和部署的 DON,这是一个高度去中心化的 DON,为多个真实世界的去中心化应用程序(dApps)提供端到端安全,以使用底层的区块链基础设施^[14]。

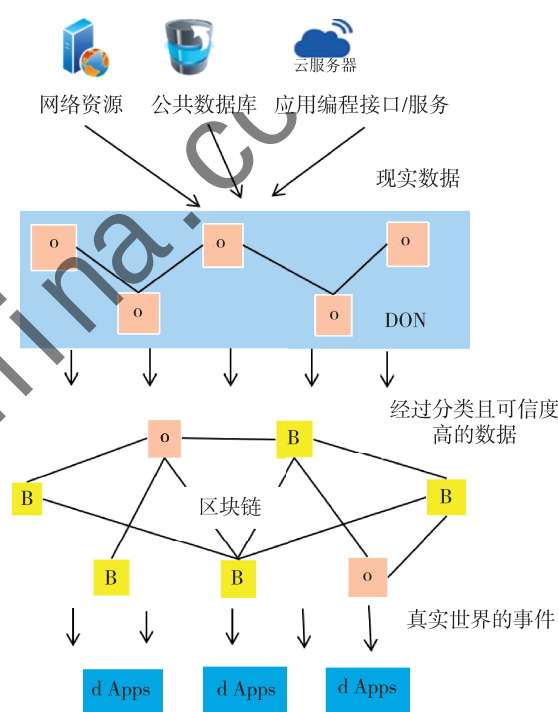


图2 DON-区块链集成支持 dApps 的总体原理

在区块链技术这种分布式账本中不需要第三方的参与,交易记录会以数据状态安全、公开保留在链上。通常情况下,智能合约的使用通常也仅限于这些链上数据,而不需要访问链外系统。但是这也解释了智能合约不灵活的原因,即智能合约与创建它们的区块链上下文之外的数据与系统完全隔离,进而造成了智能合约动态应对的能力被削弱。Blockchain's Oracle 通过将链外基础设施与链上代码结合在一起创建了复杂的去中心化应用程序(dApps),并通过开发混合智能合约,使智能合约能够基于来自现实世界的输入和输出来运行。同时,虽然 dApps 中的 DON 可以确保从不同来源获取的数据的身份验证和准确性,但仍然需要确保智能合约的正确执行,即能够

保证用户能够验证智能合约的正确执行。本文引入代理智能合约（Proxy Smart Contracts, PSC）的概念来最大程度地缓解智能合约编码错误或者测试不足的缺点。在代理智能合约系统中，首先两个相关方 A 和 B 可以使用 dApps 生态系统以 P2P 方式进行连接，决定需要由 DON 或者外部数据源加以验证，并协商执行智能合约的指定条件和财务支出。这会导致智能合约代码从现有模板中自动生成或重复使用，并安装在区块链中。与此同时，代理智能合约也会生成，以便在援引和执行真正的智能合约之前对其进行调用。当满足执行智能合约的预先指定条件时，代理智能合约就会自动被调用（如图 3 所示）。代理智能合约将区块链状态变量复制到本地状态变量中，并对本地状态变量执行所包含的业务逻辑，这确保了区块链的状态不会以任何方式被修改。并且，代理智能合约会将当前状况和预期结果行动传达给双方，如果双方提交同意书，系统就会自动援引或者执行真正的智能合约，反之如果双方提交无法达成一致，真正的智能合约不被援引或执行，则需要进行新一轮的谈判。而双方的进一步的调解可以选择自动执行或者手动执行。如果智能合约条件被验证，那么资金就会从托管账户中发放给预期方，此时部分交易也将作为临时措施记录在审计跟踪之中，并不对区块链进行修改。然而，如果验证失败，系统则会将资金进行回转，并修改审计跟踪。这样便确保了合同事务在没有通过验证时，区块链不会进行中途更新^[15]。

代理智能合约最重要的功能就是使用 DON 根据预定逻辑验证输入值，即可根据双方在谈判阶段指定的来源清单，验证 DON 上已有的其他来源的输入值。如果经过验证，则将输入值添加到训练集，以便可以更有效地检测未来的异常值。这样可以一方面为用户提供关于智能合约执行的细粒度控制机制，另一方面可以防止恶意或错误的输入值无意中影响智能合约的正确执行，并赋予智能合约双方用户当一方解除或者不履行其合同义务时，进行调解的可能性。另外，由于代理智能合约需要进行大批量的数据处理，因此为了提高代理智能合约的数据处理能力，可以将人工智能技术引入其中，从而预测智能合约是否会被执行，进而为区块链生态系统创造一个真正的信任体系结构。代理智能合约中使用人工智能模型可以促使代理智能合约做出适当的判断。例如在金融市场中，人工智能模型作为一种安全措施，通过分析和权衡安全性、吞吐量等因素检测证券交易中的违规行为，经过训练的预测股票市场价格的人工智能模型将有助于智能合约做出更好的判断。此时，如果买方希望购买卖方正在出售的所有股票，由于双方提供确认申请，

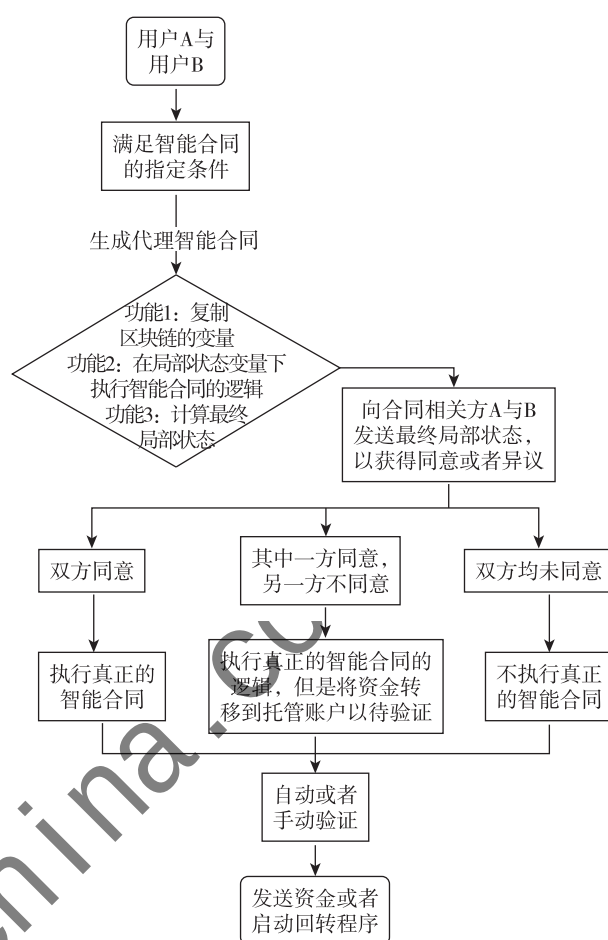


图3 代理智能合约的执行流程

此时代理智能合约就会执行真正的智能合约。如果买方只是希望购买卖方的部分股票时，买方已经收到确认申请，但是代理智能合约仍会等卖方的确认，此时资金会被发送一个托管账户，直到代理智能合约收到卖方的确认。最后，如果买房希望购买的股票数量超过了卖方希望出售的股票数量，在这种情况下，代理智能合约将不会执行底层的智能合约。

3.3 建立必要的智能合约监管系统

事实上，缺少必要监管的去中心化交易模式，会让智能合约平台提供者的权力不受约束。制约机制的缺失，使得智能合约平台提供者成为智能合约交易的唯一主宰。市场垄断、市场操纵、内幕交易等行为由此成为必然。其次，权威第三方的缺失也就意味着智能合约的交易不受到监管与控制，交易的安全性无法得到保障，甚至会成为滋生违法行为提供便利。为了能够保障智能合约交易的安全与增加信任度，在现实中需要由必要的第三方对其进行必要的介入。这里指的第三方权威既可以是国家或者政府，也可能是智能合约的提供商，也可能是合同双方共同推选出的管理者。

3.3.1 政府机构

欧盟推出的区块链监管沙盒可以很好地帮助政府机构采取“算法控制型”与“算法设计型”的两种路径去规制智能合约所带来的风险。首先,“算法控制”意味着政府的价值在于辅助智能合约成为更加稳定的应用,通过法律按照规范架构、行为框架和概念描述框架的类别予以代码化,从而便于智能合约的调用^[16]。同时,政府作为信息的掌握者,可以通过建设完备的政府数据开放系统,并与智能合约的应用端口相连接,从而为智能合约提供足够的信息支持,最大限度地解决智能合约预测性不足、灵活性不够的问题。但是这种路径也将政府过于工具化,从而使其失去了有效监督智能合约的地位。其次,如果说弥补智能合约的漏洞是以辅助智能合约运行行为目的,那么监管智能合约运行的路径则是真正意义上从规制的角度对智能合约的使用加以限制。在这种路径下,政府可以在智能合约使用前对其使用加以规范,并在智能合约的运行过程中监督其使用状况,必要时还可以借助代码规避风险^[17]。

3.3.2 智能合约平台提供者

在智能合约的实际操作过程中,智能合约平台的提供者并不直接参与智能合约的签订,只是提供必要的区块链与智能合约使用技术与使用平台。由于“算法权力”的必然,智能合约以算法为架构技术,该算法本身就是一种行为与交易规范,决定着智能合约的交易模式,由此形成平台提供者天然的管理者地位。因此,此时的智能合约平台的提供者可以类比《电子商务法》中的电子商务经营者,并且平台提供者在智能合约交易中的地位也是二元的。作为电子商务经营者的平台提供者,其需要受到《民法典》和《电子商务法》有关电子平台相关规范的约束,平台应对其参与的监管事务承担一定的注意义务和私法责任。另外,如果因为智能合约平台的设计问题导致合同当事人之间无法正常履行合同的,智能合约平台因为基于缔结的服务合同约定承担违约责任。如果是智能合约平台提供者故意或过失修改智能合约导致当事人受有损失的,发生请求权竞合,合同当事人既可如上文所述寻求违约责任救济,也可借助侵权行为、侵权的故意/过失、损害结果以及因果关系四要件的证明寻求侵权责任赔偿。总而言之,智能合约平台提供者作为一个私主体,需要确保合同当事人财产不受到侵害,并且也要设置和完善相应的事后权利救济机制。

3.3.3 区块共同选择的管理者

区块链由区块构成,并且每个区块都是一种交易主体,同时承担着记录交易信息的职责。智能合约采取的这种分布式的商业模式实际上就是依靠程序算法构建了一个自治组织,如果要为这些自治组织挑选出权威中心,

则必须尊重每个区块的意思。为此,链极智能科技(上海)有限公司已经给发明一种自主管理的方法——通过区块链公链管理联盟链成员。即在公链上创建一个智能合约,用于储存联盟链的成员信息。成员的每次交易都需要在公链上发送交易调用信息,才能实现特定更改,以完成交易。由此,区块共同选择的管理员便有了管理智能合约交易的必要权限。然而,这种区块共同选择的管理员却往往不具有技术优势与资金支持,其更适合作为平台管理者这种权威中心的辅助主体。

3.4 完善智能合约执行解决机制

如果从互联网接收到的数据损坏或处理不准确,智能合约的运行可能受到影响。因此,如何在执行背景下解决智能合约的纠纷问题就成了智能合约事后风险审查的重要环节。针对这一问题,加拿大最高法院近日提出可以将区块链 TOU 协议作为执行智能合约时具有约束力和可执行性的依据。其中,区块链 TOU 协议是指用户访问和使用通过区块链网站提供服务的信息条款,其可以作为一份独立的合同协议填补智能合约无法涵盖的空白(例如保密性或赔偿问题)。同时,TOU 协议可以被归类为附随合同,这类合同的一个共同特点就是,它们是在接受或放弃的基础上提供的,而当事人对合同的默许被视为对合同条款的接受。除非另有规定为不可强制执行,否则附随性合同具有法律约束力。基于此,加拿大最高法院认为如果区块链 TOU 协议与智能合约之间存在关系,那么基于区块链 TOU 协议可以解释双方之间合同关系的范围,则有助于解释或执行智能合约。同时,智能合约是在“If/Then”的基础上执行的单方面协议,为了强制执行单方面协议,加拿大最高法院指出必须审查智能合约与合同双方已经签署的相关协议的关系,以确定这些协议是否有助于帮助法院了解合同双方的真实意愿。如果区块链 TOU 协议与智能合约之间密切相关,法院则可以将(智能合约)单方面合同视为与该合同有关的双边协议的一个条款,这可能意味着单方面合同下的义务符合合同订立之初双方真实的意思表示,因此智能合约仍然可以执行。在 *Sail v Labrador Ltd* 案中,加拿大最高法院就当双边协议与单方面协议争议有关系时,不履行单方面合同是否会使合同不可执行提供了指导。加拿大最高法院认为租赁合同是双方签订的双边协议,但是,当事人购买租赁船舶的选择则是一个单方面的协议。并且,该双边协议要求按时支付租赁款项,并应出租人的要求,承租人应当提供账户以供检查,这些都是双边协议规定的基本义务。加拿大最高法院分析了导致租赁付款延迟和未向出租人提交记录的实际情况,发现承租

人的延迟可以得到合理解释。因此,通过将购买选择权视为双边租赁协议的一部分,加拿大最高法院也认为承租人实质上履行了合同并可强制执行。

与此同时,由于现阶段关于用户与区块链之间的法律关系类型较少,因此目前区块链 TOU 协议的内容大多数都是模糊且难以理解的,这也就可能影响区块链 TOU 协议的有效性,进而导致了法院需要主动审查用户是否已经被通知并接受其条款和使用该服务,并在法律中明确审查区块链 TOU 协议与法院的管辖权之间的关系,从而保证裁决的正当性。同时,加拿大的判例法和立法也表明,加拿大法院有权决定区块链 TOU 协议中的仲裁条款是否为有效的协议,是否应予以执行。如果这些交易是面向 B2C 的,并影响到加拿大的社会公共利益,那么加拿大法院将可以突破仲裁相对性的限制,获得管辖权并仔细审查智能合约和区块链 TOU 协议中的仲裁条款。

4 结论

毫无疑问,智能合约与 ChatGPT 等一系列新兴技术的发展,在减少合同管理过程中人为因素的同时,自然语言与计算编码之间的转换关系的不确定性也增加了合同自动化与现行法律制度的不兼容性。英美法系的判例法模式给予了较强的法律弹性,合同自动化所带来的新的法律问题可以实现在现有的合同法框架内得到处理。然而,对于大陆法系的国家而言,成文法的相对封闭性与稳定性则是为合同自动化在亚洲国家的发展蒙上一层阴影。因此,需要寻找一条适合本国国情的合同自动化的发展道路,在法律科技市场中获得更大的竞争优势。

参考文献

- [1] BLYCHA N, GARSIDE A. Smart legal contracts: a model for the integration of machine capabilities into contracts [J]. SSRN Electronic Journal, 2020. DOI: 10. 2139/ssrn. 3743932.
- [2] 王迪, 朱岩, 陈娥, 等. 智能法律合约及其研究进展 [J]. 工程科学学报, 2022 (1): 68-81.
- [3] BROOKE L. SAE and ISO refine the levels of driving automation [J]. Automotive Engineering, 2021 (5): 8.
- [4] 夏庆峰. 智能合约的法律性质分析 [J]. 东方法学, 2022 (6): 33-43.
- [5] DAN HENDRYCKS. CUAD: an expert-annotated NLP dataset for legal contract review [C]//35th Conference on Neural Information Processing Systems (NeurIPS) Track on Datasets and Benchmarks, 2021.
- [6] 陈吉栋. 智能合约的法律构造 [J]. 东方法学, 2019 (3): 18-29.
- [7] JANUARITA R, SUMIYATI Y. Legal risk management: can the COVID-19 pandemic be included as a force majeure clause in a contract? [J]. International Journal of Law and Management, 2021, 63 (2): 219-238.
- [8] REYES C L. A unified theory of code connected contracts [J]. The Journal of Coporaton Law, 2021 (4): 982-1000.
- [9] 程乐. 双层结构下智能合约条款的建构路径 [J]. 法学评论, 2022 (2): 53-66.
- [10] SCHMIDTt-KESSEN M J, EENMAA H, MITRE M. Machines that make and keep promises-Lessons for contract automation from algorithmic trading on financial markets [J]. Computer Law & Security Review: the International Journal of Technology Law and Practice, 2022, 46 (9): 24-26.
- [11] PAPANTONIOU A A. Smart contracts in the new era of contract law [J]. Limited Liability Company Commonwealth, 2020 (4): 8-24.
- [12] GAMBINO A, STAZI A. Contract automation from telematic agreements to smart contracts [J]. The Italian Law Journal. 2021, 6 (2): 35-42.
- [13] 郭少飞. 区块链智能合约的合同法分析 [J]. 东方法学, 2019 (3): 4-17.
- [14] GALLEGO-MADRID J, SANCHEZ-IBORRA R, RUIZ P M, et al. Machine learning-based zero-touch network and service management: a survey [J]. 数字通信与网络 (英文版), 2022, 8(2): 19.
- [15] GUPTA A, GUPTA R, JADAV D, et al. Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications [J]. Computer Communications, 2023 (206): 10-21.
- [16] 赵精武, 丁海俊. 论代码的可规制性: 计算法学基础与新发展 [J]. 网络法律评论, 2016, 19 (1): 97-112.
- [17] 余成峰. 法律的“死亡”: 人工智能时代的法律功能危机 [J]. 华东政法大学学报, 2018 (2): 5-20.

(收稿日期: 2023-05-23)

作者简介:

唐子晗 (1998-), 男, 硕士研究生, 主要研究方向: 竞争法与计算法学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.cn