数字人民币智能合约的风险规制

柯　达

摘要：智能合约具备自动执行、难以篡改等特点，其在我国制度环境下存在诸多应用困境。由于数字人民币表现为加密字符串，被存储于数字钱包之中，并具有国家信用的不可变更性和保管后的不可利用性，其可通过红包抵扣消费、定向汇款与调控、预付资金管理等领域的“条件支付”，改善智能合约的应用困境。但是，数字人民币智能合约仍存在法律风险，既有法律在合约拟定环节防止智能合约滥用的准入条件、审核标准以及管理义务等方面有待完善，在资金锁定与释放环节则面临数字钱包的合法性疏漏。不过，智能合约未直接限制数字人民币的货币本体，而是通过数字钱包限制支付指令的接收和发出，因此不损害货币的统一性与法偿性。对此，应在合约拟定环节构建智能合约的准入与日常管理机制，包括审核智能合约的合法性与法律语言转化、为央行的临时性干预提供技术接口等，并在资金锁定与释放环节建立小额匿名与结构化共存的数字钱包法律定位。

关键词：数字人民币；智能合约；预付资金；法偿性；可编程性

DOI：10.19836/j.cnki.37-1100/c.2024.02.016

数字人民币智能合约，是指将智能合约（smart contract）技术应用于数字人民币的发行流通，从而在市场交易、行政费用征缴等资金流转过程中实现自动化的“条件支付”或“定制化支付”，使数字人民币具备“可编程性”（programmability）[①]。数字人民币是中国版“法定数字货币”（Central Bank Digital Currency），可编程性已成为众多国家或地区研发法定数字货币的重点考量因素[②]。

据中国人民银行（以下简称为“我国央行”）于2021年发布的《中国数字人民币的研发进展白皮书》显示，数字人民币具有可编程性，通过加载不影响货币功能的智能合约，收付款人可根据约定的条件或期限进行自动支付交易[③]。一方面，与以担保为代表的经济手段和法律纠纷解决机制不同，智能合约可以在事前通过技术手段，降低相关交易的履约成本和违约风险；但另一方面，智能合约不仅存在法律性质不明、安全可靠性存疑等传统问题，而且还引发了损害货币统一性或法偿性等疑虑，进而可能对国家行使货币发行权带来不利影响[④]。因此，在加快建设金融强国、做好数字金融“大文章”的政策背景下，如何对数字人民币智能合约体现的合法性、货币流通等风险予以规制，需要在理论上予以进一步阐释。

目前，域外学界已对法定数字货币加载智能合约的技术可行性和实施方案进行分析，同时对智能

基金项目：司法部法治建设与法学理论研究部级科研项目“利益衡量视角下数字人民币的个人信息保护研究”（22SFB5049）。

作者简介：柯达，华东政法大学经济法学院副研究员，法学博士（上海 200042；zjjykeda1994@126.com）。

① 相似的概念还包括智能货币（smart money）、条件支付（conditional payment）、智能货币（smart money）。

② Bank of Canada, European Central Bank, Bank of Japan, et al., *Central Bank Digital Currencies: Foundational Principles and Core Features*, 2020, p. 8, https://www.bis.org/publ/othp33.pdf, 访问日期：2023年11月30日；Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*, 2022, p. 14, https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf, 访问日期：2023年11月30日。

③ 中国人民银行数字人民币研发工作组：《中国数字人民币的研发进展白皮书》，http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4293590/index.html，访问日期：2023年11月30日。

④ Sandner P. G., Schulden P., Grale L., et al., *The Digital Programmable Euro, Libra and CBDC: Implications for European Banks*, https://ssrn.com/abstract=3663142, 访问日期：2023年12月12日。

合约损害法定数字货币的法偿性表示了担忧[①]。国内学界已对智能合约的法律性质、安全风险等问题进行了深入研究，主流观点均认为，智能合约其意图实现的技术自治即“代码即法律”难以实现，因此需要法律干预[②]，但尚未在数字人民币领域内探讨相应的智能合约风险。基于此，本文先梳理智能合约的起源发展和既有应用困境，并在明晰数字人民币运行机制、智能合约应用领域的基础上提出数字人民币智能合约的创新之处，分析相应法律风险并提出法律完善建议。

一、数字人民币智能合约的应用创新

（一）智能合约的起源发展与应用困境

作为一种计算机程序，智能合约的产生和发展旨在消除违约的可能性进而降低履约成本。智能合约概念由尼克·萨博（Nick Szabo）于20世纪90年代提出，随着比特币的诞生和以太坊网络的发展，智能合约可以在区块链的去中心化环境下运行，由此减少对中心化主体的信任依赖[③]。典型的智能合约体现为“If-Then”的附条件执行模式，即双方当事人事先拟定履约条件和行为，当条件被满足“触发”后，计算机会自动执行履约行为。与常规合同以及其他计算机程序相比，智能合约具有以下特殊性：其一，满足条件后的自强制或自执行性。智能合约的核心条款结构体现为“预设条件-满足条件后自动执行”，这使得在条件满足后，无须双方当事人实施任何具体行为，合同亦能履行完毕[④]。其二，对特定财产或行为的可锁定或可控制性。计算机系统可在条件满足之前将特定财产进行锁定或限制实施某行为，从而强化对财产权的保护[⑤]。其三，去中心化前提下的可验证性与难以篡改。与公有链或联盟链相结合，当事人拟定的智能合约需要“上链”经各个节点验证和存储，加载成功后亦可反复验证真伪[⑥]。

智能合约虽然可实现自动化执行，并借助区块链而具有难以篡改性与可验证性，但在我国制度环境下仍存在技术和法律困境，导致应用范围较为有限。在技术层面，智能合约的标准化与自强制性使其天然缺乏合同条款变更或救济的渠道。当事人只能将表述较清晰确定的条款编入智能合约，而一些有必要进行模糊处理的条款则很难编译为合约代码；此外，自动执行后相关财产权益的变动不可撤销，但如果智能合约存在技术漏洞甚至遭受网络攻击，在缺乏外部临时干预的情况下，当事人便难以获得权利救济。智能合约的技术困境也造成其在法律上的性质难以界定，同时其体现的去中心化色彩与既有金融监管体制相冲突。一方面，智能合约是否可直接认定为法律上的合同仍存争议。例如有学者将智能合约分为合意型、先意型和实践型三类，对于先意型而言，智能合约仅仅是合同的组成部分而非全部内容[⑦]。另一方面，在国外，大量智能合约被应用于加密货币，因此智能合约应用极易与私人发行货币相联系，其不仅挑战国家货币发行权和严格金融管制，更不利于引导社会资金向实体经济流动。此外，在商业层面，尽管智能合约通过类似于担保的增信功能提升了合同履行的确定性，

① European Commission, *Eurogroup Statement on the Digital Euro Project*, https://www.consilium.europa.eu/en/press/press-releases/2023/01/16/eurogroup-statement-on-the-digital-euro-project-16-january-2023/, 访问日期：2023年12月14日。

② 王延川：《智能合约的构造与风险防治》，《法学杂志》2019年第2期。

③ 智能合约虽然在区块链技术出现之后得到广泛应用，但由于区块链技术在本质上属于分布式网络、加密技术、智能合约等技术集成的新型“数据库软件”，其与区块链技术不存在绝对的种属关系。Lee A., “What is Programmable Money?”, *Federal Reserve Notes*, 2021, https://www.federalreserve.gov/econres/notes/feds-notes/what-is-programmable-money-20210623.html, 访问日期：2023年12月12日。

④ 陈吉栋：《智能合约的法律构造》，《东方法学》2019年第3期。

⑤ 倪蕴帷：《区块链技术下智能合约的民法分析、应用与启示》，《重庆大学学报（社会科学版）》2019年第3期。

⑥ 刘薇：《区块链智能合约的法律性质》，《法治论坛》2020年第2期。

⑦ 宋云婷、沈超：《法的介入：智能合约纠纷的司法救济》，《北京航空航天大学学报（社会科学版）》2022年第6期。

但其他主流信任机制基于实施成本等因素依然有存在的必要,例如登记、失信惩戒、第三方支付备付金等①。

在此情况下,虽然智能合约较适合应用于标准化程度高、自动化和受信任需求强的金融支付领域,但受我国金融监管体制的影响,智能合约仍无法在该领域得到广泛应用。目前,我国智能合约的主要应用领域为特定非交易行为的有条件实施或信息的有条件共享,例如最高人民法院大力推动的区块链司法建设②。

(二)数字人民币的运行机制

在我国智能合约应用困境得到清晰展现的情况下,以数字人民币作为支付对象的智能合约应用存在多大的竞争优势,便有了充分的现实依据。我国央行计划将数字人民币设计为由指定商业银行作为运营机构参与运营、与实物现金等价、具备可控匿名功能的法偿货币;其中,与智能合约密切相关的运行机制是数字人民币的本体特征和发行运营模式。

在本体方面,数字人民币表现为加密字符串,被存储于数字钱包之中,并具有信用恒定性与保管后的(第三方)不可利用性。首先,数字人民币的表现形态为可变的加密字符串,其体现了"数字人民币"APP(以下简称为"数币APP")内资金余额、所有者标识、货币编号等信息。通过手机银行APP、他人转账等方式收款均会生成不同的加密字符串,以体现不同的资金来源。在加载智能合约之后,合约代码便会嵌入加密字符串,从而使数字人民币实现可编程和更强的可追踪性。其次,数字人民币被保管于差异化的数字钱包之中。数字人民币兼容"账户型""准账户型""价值型"三种数字钱包。账户型需要验证个人身份信息,匿名程度最弱;价值型需验证资金余额是否充足,匿名程度最强;准账户型居中③。按照使用权限的差异,数字钱包又可以分为"母钱包"和"子钱包":用户在数币APP首次开设的数字钱包即为母钱包,用户可通过母钱包实施兑换、转钱等基本功能;此外,用户可在母钱包中开设多个子钱包,通过加载智能合约,以实现条件支付、限额或限期支付等特殊功能,而合作商业或政府机构还可据此实施资金归集或分发的财务管理④。最后,数字人民币作为体现国家信用的新型货币,具有信用不变性和第三方不可利用性。虽然数字人民币的钱包在名义上也可被称为"账户型",但该钱包即便同样由商业银行提供,钱包中的资金仍体现为国家信用,不体现在商业银行的资产负债表之中,因而无法被商业银行用于从事其他投资活动。由此可见,数字人民币更像是被存入了商业银行提供的电子保管箱,非经用户允许,任何人不得动用保管箱中的资金。

在发行运营方面,数字人民币采用批发层和零售层结合的双层型模式。在批发层,央行基于额度管理向指定商业银行发行和注销数字人民币;在零售层,商业银行为客户提供钱包开立等服务,并与其他金融和商业机构推广数字人民币的流通和场景构建。对于智能合约而言,以预付消费为例,央行负责制定智能合约的技术标准,商业银行负责向市场推广智能合约应用,并在发行预付产品的商业机构拟定智能合约内容之后发行预付产品。此外,保管、登记、支付与结算是数字人民币发行流通的重要环节,而数字人民币的支付结算系统(以下简称为"数币支付系统")具有"独立系统运行"的特征,即该系统不依赖既有的央行运营或监管的支付系统或他国支付系统,而是自成一个

① 例如,智能合约体现的标准化条款无法为当事人在合同订立生效后提供协商变更的灵活空间,其无法完全适应合同履行过程中多变的商业风险(特别是价格波动)。因此,适度的人工审核或介入作为增强信任的机制仍有必要。

② 最高人民法院拟将智能合约应用于调解协议不履行后自动触发审判或执行立案,执行案款自动发放,数据确权和交易等信息的查询核验等环节。参见《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)。

③ 单就技术角度看,"价值型"由于支持较高程度的匿名性,所需验证的数据最少,其在加载应用智能合约方面更具效率优势。参见Sveriges Riksbank, *E-krona Report: E-krona Pilot Phase 2*, 2022, pp. 30-31, https://www.riksbank.se/globalassets/media/rapporter/e-krona/2022/e-krona-pilot-phase-2.pdf,访问日期:2023年12月12日。

④ 中国人民银行数字人民币研发工作组:《中国数字人民币的研发进展白皮书》,http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4293590/index.html,访问日期:2023年11月30日。

系统独立运行。在该特征影响下，触发智能合约自动执行的信息并不直接写入数币支付系统，而是仍由相关业务系统另行处理，在满足执行条件时通过应用程序编程接口（API）等方式接入数币支付系统[①]。

（三）数字人民币智能合约的应用领域与创新优势

自数字人民币启动试点流通以来，我国央行表示可以加载智能合约，但仅限于发挥货币功能，即时间、场景、角色等条件触发的“条件支付”，通过可编程性确保交易透明、可追踪；进一步看，智能合约可构建各类主体共同参与的“开源生态平台”，推动数字人民币的更广泛流通[②]。目前，数字人民币智能合约的主要应用领域如下：

其一，红包抵扣消费。红包消费是目前数字人民币智能合约应用最为广泛的领域，在深圳、上海等城市试点过程中，央行分支机构、商业银行与地方政府开展合作，通过抽签等形式向特定人群发放数字人民币红包（以下简称为“数币红包”）。数币红包在本质上是在消费达到一定金额后的代金券，用户在收到数币红包后，可直接或抵扣部分金额后支付使用。通过加载智能合约，数币红包的使用门槛或期限、支付场景等条件可以受到一定限制，同时还可提升商业机构的精准营销能力[③]。

其二，定向汇款与调控。一方面，在科研经费、财政补贴、工资发放等涉及公共利益的领域，由商业银行为资金发放者代发资金，以避免资金被第三方截留、挪用[④]。例如，雄安新区开展农民工工资穿透式代发，其通过智能合约限制货币持有主体，即便数字人民币从总包企业先发至分包企业、再发至个人，但分包企业仅能查询、无法截留该笔资金[⑤]。另一方面，我国央行、财政部或其他政府部门为通过数字人民币提升宏观调控的精准性，可通过对相应资金设置智能合约限制使用主体、用途或金额[⑥]，甚至可通过利率设定使数字人民币变为广义货币（M2）。

其三，预付资金管理。商业银行与特定商业机构合作发行预付费、押金等易形成资金池的服务，以避免在提供相应服务前不当挪用资金。数币APP中的预付资金管理服务被称为“元管家”，用户选择特定商户并购买受智能合约保障的预付产品后，相关资金被锁定；当用户完成消费后，商户可以发起执行智能合约的请求，系统在检查执行条件后会将相应资金划转给商户。以教育培训为例，用户在使用数字人民币缴费后，相关资金被锁定；在每完成一次课程后，加载于钱包的智能合约便会将一节课程的资金转移至培训机构的钱包[⑦]。

其四，自动化结算。具体又分为智能支付和批发资金结算。前者指商业银行为需要定期缴纳费用的客户进行自动扣款，以提升缴费便利性和加快收款人的到账时间。例如，国网雄安公司推出数币电费缴纳服务，用户的子钱包在加载智能合约、与其电户号绑定之后，可实现一个电费缴纳

① Bank of England, *Central Bank Digital Currency: Opportunities, Challenges and Design*, London: Bank of England, 2020, pp. 45-46.

② 根据我国央行相关负责人的构想，在未来，数字人民币智能合约生态服务平台会成为与手机应用市场一样的开放式平台，不同主体均可在该平台提供智能合约服务。

③ 柯达：《数字人民币的理想与现实——基于对深圳数字人民币试点活动的观察》，《金融法苑》2020年第4期。

④ Hong Kong Monetary Authority, *E-HKD: A Policy and Design Perspective*, p. 13, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/e-HKD_A_Policy_and_Design_Perspective.pdf，访问日期：2023年12月12日。

⑤ 又如，在经营银行网点成本较高、仅设置金融便民服务点的偏远地区，通过设置智能合约，由非金融机构人员为当地居民提供数字人民币的小额存取现等服务，进一步减少相关人员侵占或骗取用户资金的风险。参见中国金融四十人论坛、中国人民银行数字货币研究所：《数字人民币无障碍及包容性设计：通过无障碍及包容性设计促进我国普惠金融发展的研究》，第98页，http://www.cf40.org.cn/news_detail/12849.html，访问日期：2023年12月12日。

⑥ 姚前：《法定数字货币对现行货币体制的优化及其发行设计》，《国际金融研究》2018年第4期。

⑦ 截至2023年12月，国内已有深圳、成都等多个城市开展教培行业数字人民币智能合约的推广服务，力求解决预付资金监管的难题。

周期届满后钱包自动扣款的功能[①]。另一方面,我国央行、商业银行与境内股票等金融产品的登记结算机构或境外央行、商业银行进行合作,利用智能合约实现大批量数字人民币与金融商品之间的"货银对付"(DvP)或数字人民币与外汇之间的"银银对付"(PvP)[②]。在作为结算参与人的大型金融机构完成金融商品或资金的清算后,智能合约会按照预设条件自动完成货银对付或银银对付[③]。

在上述领域,数字人民币的创新优势集中体现于货币信用,即其彰显的国家信用及其在保管后的"不可利用性"与智能合约的"可控制性"高度契合,由此可以改善传统智能合约的应用困境。一方面,数字人民币智能合约更能有效维护客户财产权,特别是防止资金被第三方不当获取或被第三方主张其他权利。以预付资金管理为例,为了避免商家在获得客户的预付资金后进行挪用,多地出台法规或规章,通过失信惩戒、履约保证保险、资金专门存管等方式降低预付资金遭受不当挪用的风险[④]。然而,上述方式仍无法避免商家通过伪造交易记录"套取"并挪用预付资金;更为关键的是,专用存款账户仍开立在商家名下,消费者无法全面知晓某一商家的负债情况,如特定商家资不抵债进入破产程序,在存在众多优先级债权且司法机关有权对账户实施干预的情况下,消费者的预付资金债权便难以有效主张[⑤]。与监管部门直接将非银行支付机构存管于央行的客户备付金拟制为客户所有不同,在应用数字人民币智能合约之后,预付资金被数币支付系统锁定,其未进入商家的数字钱包,因此不仅消除了商家挪用资金的可能,更不会像传统专用存款账户一样直接面临优先债权人和司法机关的查冻扣影响[⑥]。

另一方面,数字人民币的国家信用属性使智能合约的"自强制性"受到国家认可,可弱化传统支付领域挑战国家货币发行权、不利于发展实体经济的质疑。在传统预付资金管理情形中,消费者提供的预付金存在两重性质,一是消费者对商家可购买特定产品或退款的普通债权,二是商家对银行的货币服务债权,二者均有一定程度上的货币属性[⑦]。由于单用途预付资金行业暂未纳入金融监管范畴,央行仍难以对其造成的多余货币供给量进行有效调控。即便将智能合约应用于存管预付资金的银行账户,相应资金仍然会受到银行信用的影响,特别是被存管于运营风险较大的银行。在此情况下,将体现国家信用的数字人民币作为智能合约的应用对象、将央行作为智能合约标准的制定者、将特定商业银行作为智能合约所依托支付系统的多中心运营者,便更有利于维护数字人民币的流通秩序和智能合约的持续应用[⑧]。

---

① 与自动缴费原理相似,资金流向相反的是"自动收款",例如,保险公司推出延误险自动赔产品,在设置智能合约之后,只要发生航班延误,用户的数字钱包便会自动收到保险公司的赔付资金。参见 Hong Kong Monetary Authority, *E-HKD: A Policy and Design Perspective*, p. 13。

② 柯达:《区块链证券结算的法律规制——基于信息系统的视角》,《大连理工大学学报(社会科学版)》2020年第5期。

③ 银行间市场清算所股份有限公司《大宗商品现货清算业务指南(2023年5月修订版)》第86条至91条;House of Lords, *Central Bank Digital Currencies: A Solution in Search of a Problem?*, p. 26, https://www.parliament.uk/business/lords/media-centre/house-of-lords-media-notices/2022/january-2022/central-bank-digital-currencies-a-solution-in-search-of-a-problem/, 访问日期:2023年12月12日。

④ "资金专门存管"侧重于事前和事中监管,其指经营者应当将预付资金存入指定银行的专用存款账户,之后银行应当根据经营者提供的交易记录进行逐笔资金划拨。

⑤ 特别是支付机构作为存款人时,由于其处于强势地位,仍然存在挪用等风险。参见中国支付清算协会编:《预付卡理论与实务》,北京:中国金融出版社,2018年,第156页。

⑥ 由此可以避免传统智能合约中,自动执行破产人财产侵害其他债权人的利益。参见夏庆锋:《区块链智能合同的适用主张》,《东方法学》2019年第3期。

⑦ 吴志攀:《金融多元化:"部门货币"问题研究》,《北大法律评论》2013年第2期。

⑧ 当然,数字人民币智能合约无法解决相关应用领域的所有纠纷或风险。以预付资金领域为例,传统的预付卡主要存在发卡主体门槛较低、预付资金遭挪用、商品服务质量低等问题,而智能合约则重在解决预付资金的监管问题。

二、数字人民币智能合约的法律风险及规制困境

（一）风险识别基础：数字人民币智能合约的法律本质界定

为更精准分析法律风险，需要将智能合约的商业逻辑转化为法律逻辑，即通过梳理支付过程和法律关系来界定数字人民币智能合约的法律本质。结合上文总结的各类应用场景、我国央行公开的专利信息，加载智能合约后的数字人民币支付过程主要分为“拟定”“锁定”“释放”三个环节[①]：其一，拟定合约模板。在遵循央行规定的智能合约技术标准的前提下，商业银行与合作商业或政府机构共同确定智能合约的具体执行条件等内容；同时，在安全可靠的环境下，将商业或政府机构的第三方业务系统中判断智能合约条件是否满足的部分与数币支付系统相连接，使得两者之间的数据实现互联[②]。其二，锁定特定资金。在用户与商业银行、合作商业/政府机构签订消费或资金结算协议之后，商业银行所运营的数币支付系统为用户创建一个挂靠于母钱包、加载智能合约的子钱包，该子钱包内的已有或将来收到的资金被锁定[③]。随后，数币支付系统向商业或政府机构的业务系统发送资金锁定的相关数据。其三，释放特定资金。在商业或政府机构的业务系统判断智能合约的条件已经满足后，该业务系统向数币支付系统发送可以释放资金的支付指令。数币支付系统在验证该指令符合智能合约中的条件内容后，便会释放用户子钱包中的资金，该笔资金的财产权转移至收款人或可供用户使用。

从以上支付过程可以发现，加载智能合约的数字人民币支付主要包含了付款人（用户）与收款人的货币给付关系，收付款人与商业银行的货币保管、扣划等服务关系，以及商业银行与合作商业或政府机构的智能合约服务与数据传输关系。其中，收付款人、商业银行、商业或政府机构在数字人民币智能合约条件下，通过支付指令或其他数据传输指令完成整个数字人民币支付过程。

在这一法律关系结构和支付行为的结构性安排下，数字人民币智能合约的本质仍然是一种计算机程序，其在法律上则体现为特定主体实施的附条件或附期限法律行为；而作为一种被“附加”的法律行为，智能合约并非限制数字人民币的货币本体，而是通过数字钱包这一保管媒介限制支付指令或其他数据传输指令的接收和发出。虽然智能合约的加载会使数字人民币的本体——加密字符串有所变动，但可体现数字人民币持有人的财产权益的核心数据结构仍然保持不变。在此情况下，智能合约主要对数字人民币的保管媒介——数字钱包施加作用，即数币支付系统接收和发出数据传输指令时，会考虑到数字钱包是否在支付金额、时间等方面被实施了相应的行为限制[④]。

（二）“拟定”环节：智能合约的准入与管理风险规制困境

在将数字人民币智能合约定性为附条件或附期限法律行为的基础上，数字人民币智能合约的法律风险可按照上文总结的“拟定智能合约”“锁定特定资金”“释放特定资金”三个环节进行分析，前者直接与智能合约相关数据的准入和审核管理有关，后两者还与数字人民币资金利用的合法性相关。

---

① 中国人民银行数字货币研究所专利：“基于数字货币的条件交易的方法和装置”（申请号：CN202111673170.2）。

② 相似的是，英格兰银行曾将智能合约系统与法定数字货币的支付系统的互联方式分为直接嵌入核心分类账、建立单独的智能合约系统、采用由第三方提供的智能合约系统这三种类型。参见 Bank of England, *Central Bank Digital Currency: Opportunities, Challenges and Design*, 2020, p. 29。

③ 陈果静：《预付费智能合约产品“元管家”发布——数字人民币场景创新提速》，《经济日报》2022年9月14日，第7版。

④ 瑞典央行亦认为，法定数字货币的可编程性意味着“有条件支付”而非“有条件货币”，后者可能会侵犯个人隐私；欧洲央行认为法定数字货币可以通过智能合约实现有条件支付，但不能使其成为“可编程货币”（programmable money）。Sveriges Riksbank, *E-krona Report: E-krona Pilot Phase 3*, pp. 5, 23, https://www.riksbank.se/en-gb/payments--cash/e-krona/e-krona-reports/e-krona-pilot-phase-3/，访问日期：2023年12月12日；European Central Bank, *Progress on the Investigation Phase of a Digital Euro: Third Report*, p. 11, https://www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov230424_progress.en.pdf，访问日期：2023年12月12日。

如上文所言,拟定智能合约模板需要央行、商业银行等多方主体的参与。在传统上,智能合约交易的完成需要依赖于区块链平台提供者、智能合约制作者、交易验证者等主体①;而由于数字人民币的发行、智能合约的审核监督需要依赖商业银行,同时对外部数据真实与安全性的保障还需要依赖商业或政府机构,因此数字人民币智能合约还体现了金融、商业或政府信用,由不同主体引发的风险更为多元。为了在发挥智能合约优势的同时兼顾运营成本和其他公共利益,智能合约的应用范围和过程应受到一定约束,对其实施准入与日常监管势在必行,但既有规制均存在一定的不足。

从准入视角看,可加载智能合约的领域范围以及审核主体范围在既有实践与立法中仍不明确。一方面,目前数字人民币智能合约的应用试点领域集中于红包抵扣消费、定向汇款与调控、预付资金管理等需要提升支付效率或资金安全的领域,虽然这些领域相关的资金流转与保管行为均已受到相应法律规范的约束(例如上文提及的预付资金存管于银行账户)②,但智能合约的法律定位暂未明确,其应用优势亦尚未得到法律认可。鉴于智能合约技术性和专业性较为复杂,将上述领域的数字人民币智能合约应用统合为同一部法律法规,作为相应领域的特别法十分必要。同时,目前试点阶段的数字人民币智能合约大致区分了几类场景领域,但该领域内加载智能合约的具体条件缺失,因此可能会导致智能合约的"滥用"。另一方面,目前对智能合约进行审核的主体是作为指定运营机构的商业银行,如未来将非指定的商业银行甚至非银行支付机构等主体纳入其中,如何差异化安排其准入监管条件仍值得进一步考量。

从日常管理视角看,首先,商业银行的具体审核标准仍待细化。通过央行相关负责人的表述立场可知,我国央行目前更强调的智能合约的审核标准为合法性(即有效性)与通用性(即一致性),特别是智能合约应满足较高的技术安全标准和反洗钱要求。不过,结合数字人民币的技术特性,诸如第三方业务系统对数币支付系统的间接安全影响、"技术-商业-法律"语言的转换是否适当等因素同样需要考虑其中。此外,由于第三方业务系统提供的数据体现了商业或政府的信用,基于维护国家信用和商业银行信用的需要,指定商业银行是否有对外部数据的复核权仍待商榷,即商业银行原先在部分领域存在的资金存管、资金监督义务是否完全被智能合约所代替。

其次,商业银行的网络和数据安全保护义务配置不明。传统的智能合约通过区块链技术而具有难以篡改和可验证的特性③,但此种因去中心化实现的"代码之治"仍存在诸多缺陷,例如缺乏法律或政府的直接介入空间④。而对于未全面采用区块链技术的数字人民币而言,其存在的天然可干预性可避免传统智能合约的诸多缺陷,但同样也弱化了因高度去中心化所带来的难以篡改和可验证优势,因此,如何为商业银行合理配置网络安全保护义务,从而实现交易的"防抵赖"以及防止合约编写错误等事由导致的程序故障至关重要。

最后,商业银行和央行的个人信息保护义务有待强化。为了便于加载智能合约以及出于反洗钱的需要,商业银行势必要处理具有一定实名程度的个人信息,但这与数字人民币意图实现的高强度隐私保护目标存在一定冲突,进而引发个人信息被不当泄露的忧虑⑤。对央行而言,智能合约可通过对用户资金实施负利率而完成特定的货币政策目标,由于《个人信息保护法》未对特定的国家机关处理个人信息作出规定、《中国人民银行法》(以下简称《人民银行法》)亦面临个人信息保护的缺位,我国央行需履行何种程度个人信息保护义务,才能满足现代央行制度下的央行独立性和可问责性尚存

① 李西臣:《区块链智能合约的法律效力——基于中美比较法视野》,《重庆社会科学》2020年第7期。

② 《北京市单用途预付卡管理条例》第22条、《上海市单用途预付消费卡管理规定》第15条、《非金融机构支付服务管理办法》第24条。

③ 徐忠、邹传伟:《区块链能做什么、不能做什么?》,《金融研究》2018年第11期。

④ 王延川:《智能合约的构造与风险防治》,《法学杂志》2019年第2期。

⑤ European Central Bank, *Exploring Anonymity in Central Bank Digital Currencies*, p. 6, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.mipinfocus191217.en.pdf,访问日期:2023年12月12日。

疑问[①]。

（三）“锁定与释放”环节：智能合约的合法性风险规制困境

数字人民币智能合约的“锁定”和“释放”环节均围绕货币资金的流转，其事实上对收付款人的货币财产权在短期内施加了一定限制。一方面，由于付款人是为了确保货币资金在未来的长期安全、收款人亦希望足额获取资金并实现其他公共或商业目的才使用智能合约，此种短期的财产权限制具备较充分的合理性。但另一方面，智能合约限制了数字人民币的流通，由于数字人民币仍为法定货币，是国家行使货币发行权的产物，其发行和支付流通受到国家高度管制，因此仍需考虑货币发行流通层面的合法性。

对个人而言，我国目前通过的《人民币银行结算账户管理办法》《非银行支付机构监督管理条例》《单用途商业预付卡管理办法》，分别认可由商业银行开立的银行账户、由非银行支付机构开立的支付账户以及由非金融行业经营者开立的单用途商业预付卡，作为保管和存储“货币价值”的媒介。由于数字人民币国家信用的不可变性以及更强程度的匿名性，数字钱包这一保管媒介无法归属于任何一种被既有法律所认可的货币保管媒介。由于不同合法的货币保管媒介对应了不同的开立条件、使用者的权利以及开立主体的义务，特别是开立主体的反洗钱和个人信息保护义务，在数字钱包合法性不明的情况下，如径行通过数字钱包加载智能合约、根据用户的特定身份信息实施条件支付，那么可能会给商业银行实施身份识别、大额交易或可疑交易报告、个人信息处理等行为的合规机制带来更大的不确定性。

对整体社会经济而言，加载智能合约的数字人民币通过条件限制可更有效保护收付款人的财产权，但基于数字钱包相较于银行账户等传统货币保管媒介的特殊性，智能合约对货币流通的阻碍在根本上不符合《人民银行法》所规定的“保持货币币值稳定”这一货币政策目标。智能合约通过锁定资金的方式，限制特定数字人民币的流转自由，其可保障收付款人相应资金收付目的的顺利实现，这种锁定相当于通过电子保管箱将其封装，使数字人民币成为“窖藏货币”进而暂时退出流通，其与传统的银行账户对应资金的可流通性存在根本不同。由于数字人民币采用与以往现金人民币基本相似的“100％准备金”发行方式，即商业银行向央行提交1单位的存款准备金后可获得1单位的数字人民币，因此无法像“部分准备金”制度下发放多于存款准备金数倍的银行贷款，从而限制了商业银行的货币创造能力。在此情况下，如果社会中被锁定的数字人民币越来越多，货币供应量便会更难与社会货币需求量相适应，最终引发通货紧缩[②]。

需要注意的是，虽然数字人民币智能合约在数字钱包和货币政策方面存在合法性风险，但将智能合约加载于数字人民币，不会损害人民币的法定货币地位（即统一性与法偿性）这一基本的合法性。其一，加载智能合约与人民币的统一性不存在直接联系。根据《人民银行法》《人民币管理条例》的规定，人民币的统一性不仅仅在于人民币样式的一致性，更在于发行与印制人民币权力的统一，以维护国家对货币发行权的垄断地位；为了维护人民币的统一性，法律禁止任何人伪造、变造、损毁人民币以及非法使用人民币图样，并禁止印制和发售代币票券[③]。如上文所言，智能合约通过数字钱包这一保管媒介限制数据传输指令的接收和发出，其未改变数字人民币本体的实质内容。即便对既有法律中的人民币“图样”“票券”等词作扩大解释、将非实体的货币数据纳入其中，只要由央行指定的商业银行

① Nabilou H., “Testing the Waters of the Rubicon: The European Central Bank and Central Bank Digital Currencies”, *Journal of Banking Regulation*, 2020, 21(4), p. 15.

② 虽然智能合约体现的“锁定”行为与《商业银行法》以及《民事诉讼法》等涉及财产保全的法律条文中的“冻结”行为在词义上较为接近，即“在一定时期/条件前提下不得由任何人转移资金”，但传统意义上的“冻结”对象目前主要限于银行存款账户、非银行机构支付账户，以及在刑事案件中用于实施犯罪行为的其他涉案财物工具。

③ 《中国人民银行法》第18条至第20条，《人民币管理条例》第15条、第26条、第28条。

依法审核并加载智能合约,其均不构成对人民币统一性的损害①。其二,加载智能合约不影响人民币的法偿性。货币的法偿性是特定类型的货币在民事或行政活动中对相应债务的法定清偿效力,债务人使用具有法偿性的货币进行全额支付后,即视为债务的清偿②。学界和业界曾担忧,如智能合约加载于法定数字货币,使其拥有可编程性,那么货币支付的条件便会受到限制,进而损害货币法偿性③。但与现金人民币本体的支付、法偿性的实现不一定要事先存放于银行账户不同,数字人民币必须依托于数字钱包这一保管媒介才可使用,由于智能合约加载于数字人民币后,仅限制了相关数据传输指令、未对货币本体带来实质性改变,其并不会影响数字人民币被收款人顺利接受,且相关支付条件的限制亦得到了收付款人双方的认可。

三、数字人民币智能合约法律风险的规制完善路径

(一)"拟定"环节:构建央行与商业银行为主导的智能合约准入机制

为了兼顾智能合约优势的发挥与社会运营成本、防止智能合约被无序滥用,需要构建数字人民币智能合约的准入机制,其中首先应明确智能合约服务提供者的基本权力(利)义务配置。总体而言,数字人民币智能合约的服务提供者主要包括央行、商业银行、商业/政府机构三类,在智能合约整个运作过程中分别作为技术标准制定者和监管者、审核监督者、外部数据提供者而存在,其中央行与商业银行的权力(利)配置最为重要。

一方面,由于智能合约的拟定与数字人民币形制有关,央行作为行使货币发行权的唯一主体,应作为智能合约的技术标准制定者和监管者,为智能合约的具体应用和及时风险介入提供有效保障。根据《人民银行法》《人民币管理条例》等规定,厘定货币的"形制"是货币发行权的核心内容之一,在数字时代,货币形制还包括界定货币的基本功能或效果;由于是否允许、如何实现数字人民币加载智能合约会影响其实现条件支付的效果,智能合约的基本技术标准制定亦应属于厘定货币形制这一货币发行权的核心范畴。

另一方面,由于智能合约通过作为货币保管媒介的数字钱包实施条件支付,商业银行作为数字人民币的发行中介以及保管业务的经营主体,应作为智能合约的审核与监督者,以保障用户的财产安全权。如上文所言,我国采用了央行与指定的商业银行共同参与的数字人民币发行运营模式,其中商业银行作为货币发行中介,面向个人和非金融企业提供包括智能合约在内的各类服务。加上发行运营服务的公共性,商业银行在提供相关服务时应当遵循更严格的公法标准(例如比例原则),因此其除了保管资金、执行资金锁定/释放指令之外,还应作为智能合约的审核与监督者。

在将审核与监督智能合约的主体归于作为指定运营机构的商业银行之后,数字人民币智能合约的准入规制便可集中于可加载智能合约的条件,具体包括:其一,货币流转的具体场景用途。由于不同应用场景体现的个人利益或社会公共利益有所不同,应首先将用于加载智能合约的应用场景分为商业交易、行政事务、社会保障,以分别对应民事主体之间、行政主体之间或行政主体与行政相对人之间、用人单位与劳动者之间的货币流转活动。其二,针对同一应用场景出现的风险或纠纷,既有解决法律制度未能提供类似的应对方式或可实现类似的效果。例如,民事主体之间的商业交易"涉众型"

① 业界曾质疑,对于无门槛使用、利用智能合约技术设置使用期限的数字货币消费券而言,如时间届满,该笔资金将从持有者的数字钱包中消失,这将使得货币的统一性丧失。参见 European Central Bank, *The Digital Euro: Policy Implications and Perspectives*, 2020, pp. 16-17。但需要指出的是,此种类型的数字人民币虽无门槛,但在本质上仍然属于代金券(承诺消费折扣的债权),因此仍然不会影响货币的统一性。

② 柯达:《货币法偿性的法理逻辑与制度反思——兼论我国法定数字货币的法偿性认定》,《上海财经大学学报》2020年第6期。

③ Nabilou H., "Testing the Waters of the Rubicon: The European Central Bank and Central Bank Digital Currencies", *Journal of Banking Regulation*, 2020, 21(4), p. 15.

强[①]，只有存在严重信息不对称、可能对付款人的财产权构成较大损害时（例如预付资金领域），才可使用智能合约，且此种智能合约不能仅应用于传统的银行账户之中，否则将导致与既有资金存管方式的重复建设。其三，不会对社会总体的货币供应量带来较大的负面影响。这要求被智能合约锁定的资金数额不宜过大，且锁定资金的期限不宜过长。当然，这同样需要额外的配套监管规定，例如，商业银行有充足的流动性准备，或者赋予商业银行对锁定资金相应的发行额度，在智能合约释放资金时予以抵扣。其四，第三方业务系统安全可靠。为了确保与数币支付系统数据互联的、由商业或政府机构运营的第三方业务系统在遭受技术故障等突发事件后，不会对数币支付系统带来技术安全风险，第三方业务系统需要建立与数币支付系统的防火墙技术手段，确保其在面临内外部风险时的可抵抗性。

（二）“拟定”环节：完善以审核监督和网络安全为重点的智能合约管理机制

在满足我国央行提出的合约模板化、可复制推广的前提下[②]，数字人民币智能合约的日常管理机制主要体现于商业银行应当履行的审核与监督、网络和数据安全保护以及个人信息保护义务。首先，明确商业银行对智能合约的合法性与法律语言转化两大审核内容。智能合约的合法性审核不在于需要将其认定为法律上的某种具体法律行为，而在于判断其是否符合法定的可应用条件（例如上文提及的对社会总体的货币供应量影响不大），以及在确保数字人民币小额匿名功能可实现的前提下，符合反洗钱、反恐怖活动融资等基本支付监管要求。此外，商业银行与商业/政府机构形成的智能合约应用合意是以法律语言事先形成，再通过专业人员编写的技术语言（即计算机代码）直接体现；而技术语言能否全面表达法律语言的内涵，会影响到智能合约在法律上认可的可执行性[③]。因此，为确保智能合约对应的计算机代码能够实现法律上的可执行性，商业银行应重点审核自动执行的条件是否清晰明确、有无体现较强模糊性的表述，以及为合约履行的相关救济权利如解除权、抗辩权等提供行使的可能性[④]。

其次，在将数币支付系统视为关键信息基础设施的基础上，商业银行应当履行更为严格的网络与数据安全保护义务，以及为央行的临时性干预提供技术接口。根据《网络安全法》《数据安全法》等法律法规之规定，在一般的互联网经营活动中，网络运营者应当通过实名认证、制定应急预案、开展风险评估等方式履行网络安全保护义务[⑤]。而包括数字人民币在内的所有货币形态，是社会经济活动的基本交换媒介，具有全局性和基础性，如数币支付系统遭受外部侵扰或发生故障，便可能阻碍社会各领域资金流动的正常运转，甚至危及国家安全，因此数币支付系统应当认定为法定的“关键信息基础设施”。基于此，商业银行作为网络运营者和数据处理者，还应履行设置专门安全管理机构和负责人、容灾备份、定期演练等额外的安全保护义务[⑥]。随着智能合约应用的普及，其安全可靠性对数币支付系统能否正常运营必将带来更深刻的影响，商业银行在履行相关安全保护义务时，还应考虑智能合约应用后的风险评估和风险监测。此外，允许监管者的临时性干预是有效保障网络和数据安全的手段之一，商业银行在建立数币支付系统和第三方业务系统的互联通道时，应当将央行在发生重大突发事件或重大技术故障时进行临时干预的接口纳入其中。特别是在涉众性和风险传导性极强的领域（例如证券结算），通过临时性干预中止智能合约的自动执行尤为重要[⑦]。

---

① 这类似于有学者提出的“强智能合约”，即限制于义务履行确定性较强、可重复使用、法律关系相对简单的交易场合。参见韩龙、程乐：《区块链智能合约的法律解构与风险纾解》，《学习与实践》2022年第3期。

② 曹莉、吕远编：《数字货币：概念与选择——周小川的论述与问答》，北京：中国金融出版社，2022年，第148页。

③ 此时，相较于仅起草法律合同内容、明确合同预期的缔约双方而言，商业银行的角色更接近于确保智能合约正常运作的“程序设计师”，因此自然需要承担审核法律语言的义务。参见王文宇：《探索商业智慧：契约与组织》，台北：元照出版有限公司，2019年，第315页。

④ Hong Kong Monetary Authority, *E-HKD: A Policy and Design Perspective*, p. 14.

⑤ 《网络安全法》第24条至第26条、《数据安全法》第27条至第30条。

⑥ 《网络安全法》第31条、第34条，《数据安全法》第31条。

⑦ Auer R., “Embedded Supervision: How to Build Regulation into Blockchain Finance”, *BIS Working Papers*, No. 811, p. 8, https://www.bis.org/publ/work811.pdf，访问日期：2023年12月12日。

最后,与网络安全紧密相关的是个人信息安全,商业银行应当参照国家机关处理个人信息的标准履行智能合约加载后的个人信息保护义务,而央行应强化个人信息保护的问责制。如上文所言,在双层发行模式下,作为指定运营机构的商业银行承担了面向个人用户提供数字人民币发行流通服务的货币发行中介角色,其相较于传统的现金人民币发行以及存款业务的公共属性更强,需要参照公法原则对其业务活动实施监管。因此,商业银行在涉及智能合约的数字人民币个人信息处理活动中,应参照国家机关的标准,在法定职责范围和限度内依照法定程序处理个人信息,不得违反比例原则收集过多信息,更不得向商业或政府机构违法提供额外的与实现智能合约可执行性相关的个人信息。此外,商业银行履行个人信息保护义务并不意味着央行不对个人信息承担任何的保护义务或监管商业银行的职责。在确保央行的相对独立性可实现的前提下,应当将个人信息保护纳入央行问责制的范畴,防止央行在实施特殊货币政策时与个人信息保护的利益发生冲突,从而在提供比既有货币支付系统更高隐私保护水平的同时,实现与央行独立性的平衡①。

(三)"锁定与释放"环节:构建小额匿名和结构化共存的数字钱包法律定位

数字人民币智能合约在锁定与释放资金环节体现的数字钱包合法性风险,不仅会影响智能合约的正常运行,还可能阻碍货币政策的顺利实施。对此,可统筹目前的人民币银行结算账户以及非金融支付机构提供的支付账户监管机制,并结合发行数字人民币的设计原则(即贴近于现金),首先将数字钱包(母钱包)确立为具有小额匿名特性的货币保管媒介。目前,数币APP内根据身份识别要求和交易限制的差异,将商业银行开立的数字钱包分为一类、二类、三类、四类,匿名程度最强的四类钱包通过手机号便能开立,但其在余额、单笔支付金额、日和年累计支付金额方面受到的限制最强;随着身份识别要求的加强,对钱包交易限制的程度也相应减弱②。如对数字人民币直接采用传统的银行或支付账户监管机制,将会对商业银行履行反洗钱义务等带来较大不确定性,特别对四类钱包而言,其已经不符合《反洗钱法》《网络安全法》分别规定的账户实名制和网络实名制的要求。对此,应基于数字人民币的特性为数字钱包建立独立的监管机制,并在开立条件、交易限额等方面对反洗钱、网络安全相关法律法规进行调整,以满足数字人民币小额匿名的需要。如表1所示,从资金匿名角度看,用于保管数字人民币的数字钱包与现金、银行账户、支付账户便可实现差异化的共存格局。

表1　我国不同资金保管媒介/支付形态的功能定位

资金保管媒介/支付形态类型	功能定位差异
现金人民币	"小额匿名":鼓励个人减少使用,禁止单位限额以上及非法目的使用
银行账户	"实名":不论金额多少均须身份识别,大额资金更为严格
支付账户	"小额、快捷、便民":不论金额多少均需身份识别,但小额的身份识别要求较低
(数字人民币)数字钱包	"小额匿名"+"大额实名":小额免于身份识别

资料来源:作者自制。

在确立母钱包合法、独立的货币保管媒介的前提下,可借鉴专门存款账户和Ⅱ类或Ⅲ类账户的监管思路,对用于加载智能合约的子钱包建立更独特的监管机制,从而建立结构化共存的数字钱包法律定位。首先,限制可以开立子钱包的母钱包范围。由于许多智能合约应用(例如代发工资)需要获得钱包用户的个人身份信息才可实现,因此加载智能合约的子钱包职能与已通过实名认证的一、二、三类钱包进行绑定,而无法与四类钱包绑定。此外,部分智能合约还涉及自动扣款功能,需要确保母钱包中留存较充足的余额,因此此类智能合约对应的子钱包应仅能与已绑定银行账户的一、二类钱包进

① Rennie E., Steele S., "Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency", *Law, Technology and Humans*, 2021, 3(1), pp. 6-17.

② 姚前:《数字货币与银行账户》,《清华金融评论》2017年第7期。

行双重绑定。其次，子钱包仅能用于与某一智能合约应用相关、对应商业或政府机构的资金收付，不得用于与智能合约无关的第三方的资金收付，以及将钱包中的数字人民币直接兑换为现金或银行存款，或与其他性质不同的智能合约应用混合使用。在具体制度构建上，可参照《人民币银行结算账户管理办法》中的专用存款账户规定，对子钱包的资金收付方向限制予以调整。如此一来，智能合约还可有效应用于企业内部的资金管理和企业间的频繁资金往来，通过资金归集、智能分账、对账和自动差错处理等方式，减少人工处理资金的失误，并强化各方的互信程度①。最后，对子钱包同样采取针对不同智能合约应用场景的交易限额机制。此种交易限制并不仅仅基于个人身份识别的差异性，更是考虑到减少智能合约技术故障所带给子钱包的损失，以及减少对央行货币政策顺利实施的影响。在具体金额限制上，可参照Ⅱ、Ⅲ类账户的分类监管思路，对涉及金融领域的智能合约应用，为该子钱包提供更高的母钱包转入资金或资金划拨金额上限，但要提前进行双重身份识别认证②。在为结构化共存的数字钱包提供合法性的前提下，数字人民币智能合约的信任优势、互通优势和后发优势便具有了充分的法治保障③。

四、结论

智能合约主要应用于数字人民币的红包抵扣消费、预付资金管理等领域，数字人民币体现的国家信用、不可利用性与智能合约的可控制性高度契合，可以改善智能合约的应用困境，并推动数字人民币更广泛流通。但数字人民币智能合约仍存在若干法律风险，需要从“拟定”“锁定”“释放”各环节进行规制：其一，构建数字人民币智能合约的准入机制，可加载智能合约的条件应包括货币流转的具体场景用途、既有法律制度未能对传统支付领域提供类似的应对方式或实现类似的效果等；其二，构建数字人民币智能合约的日常管理机制，例如建立商业银行对智能合约的合法性与法律语言转化的审核标准；其三，建立适应智能合约业务的数字钱包法律定位，例如将数字钱包确立为独立的货币保管媒介，并限制可以开立子钱包的母钱包范围。

如何对数字人民币智能合约实施法律规制，在本质上也反映了数字经济时代新型技术应用的适当性和法律的可介入程度。随着数字经济产业的规模化和普及化，将智能合约应用于货币支付、使货币具有可编程性的需求将会越来越强，从而刺激新型技术和商业模式的出现④。此时，如何基于收付款人的资金使用偏好差异，作出更为合理的利益平衡方式，以鼓励更多的商业或政府机构使用数字人民币智能合约、推动数字经济的深入发展，则值得进一步深入思考。

Risk-Based Regulation on the Smart Contracts in e-CNY

Ke Da
（Economic Law School, East China University of Political Science and Law, Shanghai 200042, P.R.China）

Abstract: Smart contracts, enabled by blockchain technology, are characterized by their capacity for

① 周怡君：《数字人民币担保制度框架构建》，《东方法学》2022年第2期。

② 《中国人民银行关于落实个人银行账户分类管理制度的通知》（银发〔2016〕302号）。

③ 中国人民银行数字货币研究所：《扎实开展数字人民币研发试点工作》，《中国金融》2022年第20期。

④ Bank of Canada, European Central Bank, Bank of Japan, et al., *Central Bank Digital Currencies: User Needs and Adoption*, p. 5, https://www.bis.org/publ/othp42_user_needs.pdf，访问日期：2023年12月12日。

autonomous execution, verifiability, and resistance to tampering. However, within the context of China's institutional framework, particularly its financial regulatory system, smart contracts encounter technical and legal challenges, leading to their limited application scope. The Digital Yuan (e-CNY), China's central bank digital currency, is denoted by an encrypted string and held within digital wallets, ensuring a stable credit value and safeguarding against unauthorized third-party use post-custody. Within this operational framework, the e-CNY, when integrated with smart contracts, facilitates conditional payments. These include applications such as utilizing red packets for shopping discounts, targeted remittance or macroeconomic control, advanced fund management, and automatic settlement—thereby potentially mitigating the practical difficulties faced by traditional smart contracts. When equipped with smart contracts, the e-CNY transaction process is delineated into stages of "drafting," "locking," and "releasing," reinforcing that at its core, the smart contract within the e-CNY remains a computer program. As conditional legal constructs, smart contracts do not impede the intrinsic value of the e-CNY but rather govern the receipt and dispatch of payment instructions or other data transmissions via the digital wallet, which serves as the custodial medium, thus preserving the currency's integrity and efficacy as legal tender. Notwithstanding, smart contracts associated with the e-CNY are not immune to legal perils. In the drafting phase, existing legislation lacks clarity regarding the permissible domains for smart contract integration and the auditing bodies' scope. Specifications for commercial banks' auditing standards and obligations, particularly concerning network and data security, call for further elaboration. Moreover, the responsibilities of commercial banks and the People's Bank of China (PBOC) regarding the protection of personal information necessitate reinforcement. During the locking and releasing phases, the digital wallets that house the e-CNY with smart contracts exhibit legal vulnerabilities that cannot be readily resolved through supplementary legal interpretation. To enhance the regulatory framework surrounding the e-CNY's smart contracts, the drafting phase should introduce a vetting mechanism spearheaded by the PBOC and commercial banks. Crucially, as the formulation of smart contracts is intrinsic to the e-CNY's architecture and the PBOC holds the exclusive right to issue currency, it should assume the dual role of establishing technical standards and serving as the regulatory authority for smart contracts. This would ensure robust support for their application and facilitate prompt risk intervention. In the locking phase, the management of smart contracts should prioritize audit supervision and cybersecurity, necessitating clear guidelines for commercial banks on evaluating legality and converting legal language. During the releasing phase, the legal framework should support a digital wallet structure that accommodates both small, anonymous transactions and a structured co-existence with other forms. This entails establishing a parent wallet as a legitimate, autonomous currency repository and devising a distinct regulatory approach for subsidiary wallets loaded with smart contracts, drawing inspiration from the governance of specialized deposit accounts and Type II or III accounts. Consequently, a structured coexistence within the wallet's legal positioning could be achieved.

Keywords: e-CNY; Smart contract; Advance fund; Legal tender; Programmability

[责任编辑:王玲强]