数字人民币智能合约开启智付新未来

文/狄　刚*

摘要：近年来，数字人民币稳步扩大试点范围，持续延伸服务触角，主动参与国际交流合作，在更多领域开展积极探索和创新，数字人民币智能合约也取得突破性进展。

关键词：央行数字货币　数字人民币　智能合约

一、智能合约的历史演进

在智能合约这一概念诞生以前，人类就围绕控制论和信息论作了很多有益探索。早在2000多年前，古希腊工程师赫伦·亚历山大在其著作《气体装置》里描述了一款自动售水机，在开关机制里放入钱币，相应重量的水就从售水机里流出来。他还提出了自动神庙门设计，即在神庙旁边点燃火炬，神庙门自动打开。这些是人类对控制论的第一次正式研究。300多年前，欧洲掀起了一场包括计算工具在内的计算自动化研究浪潮，微积分理论奠基者莱布尼茨发明了一款“莱布尼茨计算器”，可自动进行加减乘除四则运算。到了20世纪，自动机理论成为计算机科学的重要分支，冯·诺依曼、艾伦·图灵等计算机学家都研究过自动机，有限状态自动机是智能合约重要的业务逻辑的控制基础。20世纪90年代，智能合约概念被尼克·萨博正式提出，并经历了以下三个发展阶段。

第一个阶段是概念阶段。1994年尼克·萨博提出智能合约概念及特性，概

* 作者单位：中国人民银行数字货币研究所。本文是根据作者在2023年9月第12届中国支付清算论坛上的发言整理。

念核心含义是“以计算机代码的形式记录合同当事人承诺履行的义务，并在约定条件下由代码强制执行”，4 个特性包括可观测性、可验证性、隐私性和强制性。尼克·萨博举过一个基于智能合约实现“智能财产”的例子，若一人租赁了一辆汽车，未能按时付款，汽车内部嵌入的控制单元可以自动将汽车控制权归还给汽车所有者。由此，智能财产将只为真正的所有者提供价值，并且可以消除被盗的可能性。对于如何实现智能合约应用，尼克·萨博从信息论和系统论的角度提出智能合约应具备的 12 项能力，但当时局限于技术发展，很多能力，如多方安全计算、同态加密、隐私保护等只停留于概念阶段，并没有落地。该阶段第二个代表事件是伊恩·格里格提出李嘉图合约概念，即基于密码学技术保障的一种描述金融价值的文件。李嘉图合约可供机器和人阅读，既具有法律特征又具有可执行性，所有不同形式，无论是电脑显示还是纸质打印抑或是软件解析，都是等价且保持一致性的，有人将之称为“代码即法律，法律即代码”，是更契合金融应用需求的智能合约。李嘉图合约的一致性和合约模板是衔接智能合约和法律文本的关键点，合约模板定义了合约参数和规则，同时智能合约代码和相关的法律文本条款能够做到一一映射。

第二个阶段是技术应用探索阶段。2014 年，以太坊借助区块链等技术初步实现智能合约落地，但并未用于服务实体经济；2015 年瑞银集团提出基于智能合约的智能债券系统；2017 年麻省理工学院、伯明翰大学提出基于智能合约的学历认证系统。

第三个阶段是落地阶段，包括法定数字货币对智能合约的应用。国际清算银行在 2022 年度报告中提出关于未来货币体系的愿景，认为未来货币体系将是新技术能力与央行数字货币的卓越结合，其中新技术能力明确提及了智能合约。

总体而言，随着各种数字技术的成熟应用和发展创新，智能合约的技术体系和理论内涵不断丰富，但主导智能合约发展最重要的三大内生动力是“系统论”“信息论”“控制论”。

二、法定数字货币智能合约的发展现状与优势

英国央行在一些报告里探讨了基于智能合约的央行数字货币的创新应用，智能合约的可编程性可应用于预付费管理、DVP、物联网支付和 PVP 等场景。英国

央行还围绕基于智能合约的微支付展开讨论，在现有的支付系统中，处理小额支付的成本可能大于支付本身的价值，例如，读者订阅了一份杂志，阅读一篇文章可能需要花费几分钱，但是支付成本远远超过几分钱，此时可以通过智能合约自动支付微额费用，从而降低支付成本和提高支付效率，而这正是基于智能合约实现微支付的价值所在。

德国央行曾发布报告《从跨行业领域看德国经济中可编程应用的货币》，从德国实体经济和金融部门感兴趣的领域，介绍了基于智能合约的可编程央行数字货币的9个潜在创新用例，包括DVP支付、M2M支付、IOT支付、双向清算、离线支付、跨境支付、7×24小时自动交易、随需支付、信息流资金流统一等。

中国人民银行研发的数字人民币可以通过加载不影响货币功能的智能合约实现可编程性，使数字人民币在确保安全与合规的前提下，根据交易双方商定的条件、规则进行自动支付交易，促进业务模式创新。最近几年，教育培训机构、健身房、理发店破产倒闭、卷款跑路的事件屡见报端，使用数字人民币智能合约预付资金管理可以有效解决这一问题。消费者预付资金存管在消费者数字人民币钱包里，当消费者完成一次消费后，商户发起智能合约执行请求，智能合约检查是否符合约定的执行条件后才将一次消费金额划拨至商户，这样就不存在卷款跑路的问题了。此外，智能合约还可以在定向支付、财政补贴、科研经费、营销与零售、消费红包、跨境贸易、资金结算和归集等场景发挥潜力。

数字人民币智能合约包含五个方面特性：一致性、可观测、可验证、隐私性和自强制性。随着技术的发展，智能合约的特性已经可以通过相关技术来实现，比如智能合约与法律文本的一致性可以采用多方签名技术、规范化智能合约模板、模型仿真执行、形式化证明等技术来保障实现；可观测性可以通过数据强制性同步、可视化、数据脱敏等技术保障；可验证性则可通过签名验证、零知识证明等实现；隐私性可以通过TEE可信硬件、ZKP、同态加密等实现；自强制性可采用独立无干扰的可信运行环境、交易触发自动执行、哈希签名以及相关信息安全防护技术来保障。

数字人民币智能合约应用具备三大优势：信任优势、互通优势和后发优势。信任优势包括支付结算可信、交易环境可信；互通优势是指智能合约与外部系统实现互通、智能合约不同运行环境之间实现互通；后发优势是指智能合约是一个长期演进的技术路线，可以持续迭代、继承式发展，将前期所有的传统电子账

户、区块链、密码学知识以及现有的数字货币新技术融合为一体动态升级应用技术，不断演进业务模式和创新模式。

数字人民币智能合约有五大设计理念：第一，坚持中心化管理和双层运营的架构；第二，保持合约模板的合法性和有效性；第三，坚持开放开源；第四，持续进行技术升级，防范技术风险；第五，注意制度衔接和剩余风险防范。

三、智能合约应用前景与未来发展趋势

数字经济具有数字化程度高、资金运转效率高、创新性强等特点，这些特点导致所有的经济活动最终都离不开结算，结算就是价值交换，需要可信的支付作为支撑。而可信支付则要满足合法性、真实性、有效性和安全性四大核心需求。其中，合法性需求是第一位的，即任何一笔支付只要在国家体系内就必须保证交易背景是合法的；真实性是指交易的对象、内容、钱是真实存在且实际发生、不可伪造的；有效性是指交易达成后需强制执行、不可撤销、防止篡改；安全性是指支付信息的最小必要和保护隐私原则，同时要保证交易的安全。

可信支付的关键需求可通过智能合约及相关区块链技术创新来保障，特别是密码学技术的机密性、可认证性、不可抵赖性和完整性在其中发挥了重要支撑作用。智能合约的契约机制给数字经济带来很多价值，如降低数字经济活动的履约成本和违约风险、提升效率、保障公平等。

面向未来，智能合约有 5 个主要发展方向：第一，要致力于建立全面的自主可控的智能合约技术支撑体系。实现智能合约从开发部署、安全验证、执行、运维管理的完整 Devops 一体化流程，确保数字金融智能合约全生命周期高效与安全。第二，为满足安全性、确定性、开发者友好、图灵完备等需求，要研制自主可控的智能合约领域开发语言，通过可信构造，实现智能合约形式化模型的自动生成，再对模型流程进行仿真和形式化验证，最后生成代码。第三，智能合约和法律密切相关，要构建数字金融智能合约法律分析框架，探索特定场景中法律文本到智能合约的映射技术。一方面，研究智能合约如电子证据、自动执行等法律属性依据，研究法律文本和智能合约之间的映射关系；另一方面，为了保障原有法律文本与智能合约的一致性，需研究新的智能合约 DSL，让机器和人类可读，使用密码技术绑定法律文本和合约代码。第四，要构建软硬一体化隐私保护能

力。从伊恩·格里格到尼克·萨博，都在探讨如何平衡隐私保护和监管要求之间的关系，尤其是在算法和一系列攻击挑战之下如何保证安全性。在软件方面，目前有安全多方计算、同态加密、环签名、零知识证明等技术，硬件有 SE 和 TEE 等安全单元技术，通过软硬件结合的方法构建一整套隐私保护能力，同时满足监管要求。第五，建立多层次技术生态体系。为构建安全高效且商业可持续的生态体系，基于数字人民币中心化管理和双层运营架构，智能合约生态体系要遵循分层管理、职责清晰、开放合作的总体原则。在最底层，央行端负责提供参与方准入、合约模板注册和交易互联互通等基础设施服务；在中间层，运营机构提供数字人民币的交易、支付服务以及搭建智能合约运行环境；在最上层，其他商业机构负责搭建场景应用平台，满足千差万别的市场需求。总之，要通过多层次智能合约技术生态的建立来满足未来智能合约服务实体经济的需求。