ICS 35.240
CCS L 70

中华人民共和国国家标准

GB/T 43579—2023

区块链和分布式记账技术 智能合约生命周期管理技术规范

**Blockchain and distributed ledger technology—
Technical specification of smart contract lifecycle management**

2023-12-28 发布　　2024-04-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　概述 …… 2
5　通用技术要求 …… 2
5.1　设计开发 …… 2
5.2　编译部署 …… 3
5.3　触发执行 …… 4
5.4　维护管理 …… 6
6　通用评估方法 …… 7
6.1　设计开发 …… 7
6.2　编译部署 …… 8
6.3　触发执行 …… 8
6.4　维护管理 …… 11
附录A（资料性）　常见智能合约漏洞 …… 13
参考文献 …… 15

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国区块链和分布式记账技术标准化技术委员会(SAC/TC 590)归口。

本文件起草单位：蚂蚁区块链科技(上海)有限公司、中国电子技术标准化研究院、众安信息技术服务有限公司、深圳市前海智慧版权创新发展研究院、上海万向区块链股份公司、四川长虹电器股份有限公司、南京鑫智链科技信息有限公司、湖南天河国云科技有限公司、西南林业大学、蚂蚁科技集团股份有限公司、杭州趣链科技有限公司、深圳市腾讯计算机系统有限公司、复旦大学、工银科技有限公司、西安交通大学、南方电网大数据服务有限公司、国家应用软件产品质量检验检测中心、上海分布信息科技有限公司、达闼机器人股份有限公司、腾讯云计算(北京)有限责任公司、北京大数据先进技术研究院、上海阵方科技有限公司、浙商银行股份有限公司、上海零数众合信息科技有限公司、广州南方投资集团有限公司、永旗控股(北京)有限公司、研祥智能科技股份有限公司、京东科技信息技术有限公司、中移动信息技术有限公司、北京泰尔英福科技有限公司、工业和信息化部电子第五研究所、联通数字科技有限公司、国家工业信息安全发展研究中心、华为云计算技术有限公司、华为技术有限公司、北京大学计算与数字经济研究院、神州数码信息服务股份有限公司、国网区块链科技(北京)有限公司、上海奥若拉信息科技集团有限公司、北京微芯区块链与边缘计算研究院、中国民航信息网络股份有限公司、浙江大学、香港理工大学、广州赛西标准检测研究院有限公司、敏于行(北京)科技有限公司、恒宝股份有限公司、北京合思信息技术有限公司、深圳江行联加智能科技有限公司、深圳博思互联科技有限公司、北京国金汇德工程管理有限公司、浙江出彩智能科技有限公司 、江西开创数码科技有限公司、中国信息通信研究院。

本文件主要起草人：李鸣、闫莺、彭晋、昌文婷、周平、邱英英、杜宇、郝汉、李克鹏、欧昀、王栋、于秀明、李努锲、杨征、梁志宏、王海军、张雁、张晓蒙、蔡亮、陶立春、王绍刚、王晨辉、王威、谢辉、刘亭杉、劳卫伦、刘天成、阚海斌、笪鸿飞、龚自洪、杨国正、兰春嘉、王义、艾崧溥、相里朋、王文呈、潘妍、张子怡、张亮亮、任凤丽、杨文锋、武杨、任常锐、孙林、陈晓丰、郝玉琨、康信伟、石娜、郁岩生、谭林、黄宇翔、范铭、邬萌、邱炜伟、刘冕宸、金晓娜、梁军、钟礼斌、宋文鹏、杨珍、王鑫、王海龙、田森、包小敏、彭涛、孙琳、种法辉、张小军、曲强、李达、晏海水、杨荣霞、苏庆慧、杜娟、贾祥娟、周钢、张栋、曹建农、王保春、庞伟伟、颜爱军、钱京、樊小毅、陈冬、周子茗、张金伟、马春荃、华崇鑫、魏凯、张奕卉、石竹玉、黄德俊、秦日臻、谢云龙、郭东升、季静婷、陈志列、庞观士。

引　言

近年来，在产业政策、法律法规、技术进步、市场发展等多方面推动下，区块链技术正加速“脱虚向实”，助力实体经济高速发展。智能合约是存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本上。智能合约将区块链带入了可编程，智能化时代。然而，随着智能合约日益广泛地应用，不规范的设计、开发、测试及维护带来了许多风险问题，造成了严重损失。

为了给应用区块链联结的各行业、各企业和相关组织提供可实施的标准，本文件对区块链智能合约的生命周期进行了深入的分析，梳理了智能合约生命周期各阶段，包括设计开发、编译部署、触发执行和维护管理。在生命周期的各个阶段，本文件提炼需要遵循的相关要求，从而构建出一套可实施的，能够避免智能合约可能出现风险的执行流程，为区块链联结的各个行业提供可操作、具有指导意义的智能合约实施规范。

区块链和分布式记账技术
智能合约生命周期管理技术规范

1 范围

本文件规定了智能合约生命周期中设计开发、编译部署、触发执行、维护管理等环节的技术要求，描述了各环节的评估方法。

本文件适用于区块链相关方开展智能合约的建设、应用和审计。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块链 blockchain

使用密码链接将共识确认过的区块按顺序追加形成的分布式账本。

注：区块链被设计用来抵抗篡改，并创建最终的、确定的、不可变的账本记录。

[来源：GB/T 43572—2023，3.6]

3.2

智能合约 smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本中。

注：智能合约可以在法律上代表合同条款，并在适用司法管辖区的法律下产生可强制执行的义务。

[来源：GB/T 43572—2023，3.72]

3.3

数据类型 data type

规定数据结构的数据对象的经定义的集合和一组许可的运算，在这些运算中任何一个执行时，其中数据对象都当作运算数。

[来源：GB/T 5271.17—2010，17.05.08]

3.4

形式化验证 formal verification

通过对算法逻辑的数学形式化表达，验证智能合约程序确定性和完备性的方法。

3.5

预言机 oracle

使用分布式记账技术系统外部数据更新分布式账本的服务。

[来源：GB/T 43572—2023，3.28]