**国家标准《信息安全技术 区块链技术安全框架》**

**（征求意见稿）编制说明**

**一、工作简况**

* 1. 任务来源

本标准由国家标准化管理委员会2020年下达的国家标准编制计划，项目名称为《信息安全技术 区块链技术安全框架》，计划号：(20210998-T-469)。计划项目类型为标准制定，项目牵头单位为清华大学。该标准由全国信息安全标准化技术委员会归口管理。

* 1. 主要起草单位和工作组成员

该标准编制团队由清华大学牵头，标准应用推广牵头单位是中国人民银行数字货币研究所。蚂蚁科技集团股份有限公司、京东数字科技控股有限公司，北京百度网讯科技有限公司、杭州秘猿科技有限公司、深圳市纽创信安科技开发有限公司、山东大学、山东区块链研究院、阿里云计算有限公司、华为技术有限公司、鼎链数字科技（深圳）有限公司、浙江大学、矩阵元技术（深圳）有限公司、中国电子技术标准化研究院、国家信息技术安全研究中心、深圳市腾讯计算机系统有限公司，共同参与了该标准的起草工作。

* 1. 主要工作过程

1. 2020年1月- 4月，研究国内外区块链安全相关标准，为本标准的编制奠定基础，包括：国际ISO/IEC，ITU-T，IEEE等，以及国内区块链相关的行业和团体标准；调研国内相关领域的标准，如GB/T 31168-2014 与网络安全等级保护2.0；GB/T 37092《信息安全技术 密码模块安全要求》，讨论区块链安全规范重点内容摘要等 。成立编制组，召开项目申报启动会，讨论明确标准撰写思路，编写标准草案；在编制组范围收集标准反馈意见，组织6次标准研讨会；形成标准草案。
2. 2020年5月-7月，在全国信安标委2020年第1次会议周上做立项汇报，征集标准草案意见，根据成员单位的反馈意见，对标准文本进行了修改完善。
3. 2020年8月-9月，完成任务书编制，征集参编单位，组建标准编制组。召开项目启动会，针对项目中的重点和难点集中讨论，对标准文本认真研究讨论，集中处理收到的意见。
4. 2020年10月，参加重点项目审查会议、SWG\_BDS工作组讨论会，征集标准草案意见。清华大学负责意见汇总，召开标准编制会议，对标准文本认真研究讨论，集中处理收到的意见，完善标准草案。
5. 2020年11月-12月，在全国信安标委2020年第2次会议周上做标准草案编制汇报，征集标准草案意见，根据成员单位的反馈意见，对标准文本进行了修改完善。
6. 2021年1-4月，参加重点项目审查会议，组织区块链技术安全框架标准专家研讨会，以及邀请专家对标准文本进行审核，征集标准草案意见，根据专家意见，对标准文本进行了修改完善。参加标准试点工作部署会，准备标准试点方案。
7. 2021年5月，在全国信安标委2021年第1次会议周上做立项汇报，征集标准草案意见，根据成员单位的反馈意见，对标准文本进行了修改完善，起草标准试点方案草案。邀请专家对标准文本进行审核，对标准文本认真研究讨论，集中处理收到的意见，完善标准征求意见稿。
8. 2021年6-7月，参加重点项目审查会议，组织征求意见稿研讨会议，邀请专家对标准文本进行审核，集中处理收到的意见，完善标准征求意见稿。完善标准试点方案，并开展试点工作。

**二、标准编制原则和确定主要内容的论据及解决的主要问题**

* 1. 标准编制原则

(1) 本标准严格遵守《中华人民共和国密码法》、《中华人民共和国网络安全法》、《区块链信息服务管理规定》等法律法规的要求，针对国内区块链信息服务，提出区块链技术安全框架。密码技术应用和安全管理遵循国家密码相关国家标准和行业标准，在密码技术方面也推荐相关的国际ISO标准。

(2) 本标准立足于当前国内区块链服务系统或网络的实际状况，针对区块链存在的安全风险，充分调研学术界的最新成果和产业界的实践，提出区块链技术安全框架，从根本上保障区块链服务的安全性。本标准针对区块链的安全架构，从区块链安全战略、区块链安全技术、区块链安全管理运行和区块链安全基础对区块链系统或网络提出了基本安全要求。

(3) 本标准适用于指导基于区块链技术的信息系统进行安全风险防范，特别是联盟链系统；适用于指导区块链业务提供者和技术提供者按照区块链技术安全框架设计、开发、研制、部署、运行和维护区块链，指导所有区块链参与者在区块链研制和运行的全过程中进行整体规划、安全框架设计、及安全性评估。

* 1. 确定主要内容的论据

区块链是采用密码技术保障交易的分布式数字账本，具有难以篡改、可溯源、实现多方信任等特点，国内外区块链技术和产业正在快速发展，经过近十年的发展，已经在金融、供应链等领域探索应用。但是区块链的关键技术、核心平台和产业生态都还不成熟，实际中的区块链平台或者应用面临着严峻的安全挑战。

清华大学联合在区块链技术和区块链安全方面均有代表性的单位组建了编制组，一起发挥各自优势，联合开展课题攻关。课题组成员单位包括区块链安全研究的科研单位清华大学、山东大学和浙江大学在区块链安全、密码技术和隐私保护等方面具有雄厚的研究实力；央行数字货币研究所在区块链金融领域应用具有独特的优势，有助于加强区块链技术安全框架标准的应用推广和试点验证；我国区块链具有影响力的企业蚂蚁金服、阿里、百度、京东、矩阵元等具有较好的区块链应用场景。

1）通过对区块链中的安全风险进行调研，不仅包括产业方面，而且对于学术界的最新的研究成果进行了梳理，包括密码技术、共识、智能合约、隐私保护、数据安全、存储安全以及跨链等，将这些技术及其安全要求进行总结，凝练基本的要求，构建区块链技术安全框架。

2）本标准研制的过程中，通过对国际上Fabric、libra等主流的区块链平台、国内数研所、蚂蚁金服、阿里、百度、京东、秘猿、矩阵元等十多个厂家的区块链架构进行调研、分析，研讨了这些企事业单位的区块链平台、区块链系统应用项目等，制定的区块链技术安全框架符合应用场景，能够满足产业化需求。同时针对区块链技术的运维安全、监管审计以及安全管理方面都进行全面的研究，探索了以密码安全保障技术为支撑的区块链安全架构及安全管理机制。

3）本标准的编制过程中对国际上的ISO/IEC的区块链标准进行了梳理，包括正在研制的ISO/DIS 23257区块链参考架构等。调研了国内区块链监管审计方面的要求，包括网信办发布的《区块链信息服务管理规定》等，以及国内区块链相关的行业标准和团体标准，包括金标委发布的JR/T 0184—2020《金融分布式账本技术安全规范》，工信部公示的通信行业标准YD/T 3747-2020《区块链技术架构安全要求》等。

* 1. 解决的主要问题

本标准重点解决下面的几个重点和难点问题：

不同区块链的架构不同，如何兼容金融机构、企事业单位、重点行业的区块链平台，提炼出普适性的安全框架，解决区块链技术安全框架不统一的问题，为区块链服务提供商开发区块链系统，进行系统部署和维护提供参考。

如何处理区块链技术安全框架中各个层之间的关系交织，提炼各个层的安全要求的问题。

目前区块链相关的标准缺乏，国内外都在制定，存在如何与国内和国际相关标准进行衔接，以及后续推广为国际标准的问题。

通过对区块链系统面临的安全风险进行调研，针对区块链系统面临的安全威胁、风险和脆弱性等问题，提出统一的区块链技术安全框架，梳理框架的层次结构以及各个层次的交织关系，概述密码技术、基础设施、应用层、合约层、共识层、网络层、数据层、隐私保护、身份认证和管理、跨链操作、监管审计和管理运维等的基本安全要求。

本标准从用户角色和功能的角度两方面描述安全框架要求。第1章阐述本标准的适用范围；第2章列举制订本标准规范性引用的内容；第3章对本标准中术语、定义进行规定；第4章对本标准中缩略语进行规定；第5章概述了区块链技术、区块链参与角色和区块链面临的安全风险；第6章概述了区块链的安全框架，以及安全框架包含的各个功能模块；第7-9章针对区块链技术安全框架，对区块链密码支撑、区块链安全功能组件、区块链安全管理运行进行阐述，以及相应的基本安全要求。

**三、主要试验[或验证]情况分析**

暂无

**四、知识产权情况说明**

本标准不涉及专利。

**五、预期的作用和效益**

本标准针对金融领域、企事业单位等采用的区块链技术进行梳理，分析其面临的安全风险，提出区块链技术安全框架，描述了框架的层次结构以及区块链各参与角色的安全视图。本文件适用于指导基于区块链技术的信息系统进行安全风险防范，特别是联盟链系统；适用于指导区块链业务提供者和技术提供者按照区块链技术安全框架设计、开发、研制、部署、运行和维护区块链，指导所有区块链参与者在区块链研制和运行的全过程中进行整体规划、安全框架设计、及安全性评估。保障区块链技术在各应用场景下的安全应用和在各行业中的健康发展，使之避免一些已知的安全问题：如不规范的密码算法或密码协议使用带来的安全风险；因区块链系统设计缺陷或者实现漏洞带来的安全隐患，导致用户资产、用户身份、链上数据存在风险等。

**六、采用国际标准和国外先进标准情况**

本次标准术语和定义结合了ISO 22739:2020区块链和分布式账本术语，针对国内区块链应用进行完善和修订，区块链技术安全框架调研了国内外重要的区块链架构，也参考了国际在研标准ISO/DIS 23257。区块链技术安全框架中涉及到的密码技术给出了推荐的国家标准和ISO/IEC国际标准，在技术上具有先进性及前瞻性。

**七、与现行相关法律、法规、规章及相关标准的协调性**

本标准适应我国国情，本标准严格遵守《中华人民共和国密码法》、《中华人民共和国网络安全法》、《区块链信息服务管理规定》等国家相关法律法规的规定。本标准推荐区块链系统采用的对称密码算法、非对称密码算法等参考国家标准GB/T 32918、GB/T 32905和GB/T 32907以及相应的国际ISO标准；实体鉴别技术参考国标GB/T 15843系列算法；密钥管理中的对称密钥、非对称密钥、群密钥以及密钥派生等国标GB/T 17901。采用的密码模块符合GB/T 37092二级及以上的要求。区块链运行环境符合GB/T 22239三级及以上要求，区块链运维管理中的身份认证与权限管理、密钥管理等工作根据GB/T 22239和GB/T 36626中的安全运维相关要求开展运维工作。区块链中的可信时间源应满足GBT 20520时间戳系统规范。区块链系统中的要符合GB/T 37092对随机数生成和敏感安全参数生成的要求，生成的随机序列要符合GB/T 32915对随机性的要求等。

**八、重大分歧意见的处理经过和依据**

无。

**九、标准性质的建议**

根据本标准的性质，建议本标准为推荐性标准。

**十、贯彻标准的要求和措施建议**

国内目前没有关于区块链技术的安全标准。建议尽早颁布本次修订标准，为各行业应用此类标准提供指导建议。

**十一、替代或废止现行相关标准的建议**

无

**十二、其它应予说明的事项**

无。

《信息安全技术 区块链技术安全框架》编制工作组

2021-7-10