

**上海市地方标准《区块链技术安全通用要求》  
报批稿编制说明**

**上海市信息安全测评认证中心**

## 一、工作简况

### （一）任务来源

《区块链安全技术通用要求》是上海市市场监督管理局下达的2019年度第二批上海市地方标准制修订项目计划，具体来源于《上海市市场监督管理局关于发布2019年度上海市地方标准制（修）订项目申请指南的通知》（沪市监标技2019（31）号），本标准由上海市信息安全测评认证中心牵头承担，旨在指导基于区块链技术的產品或应用的安全设计、开发、测试及维护。本标准由上海市经济和信息化委员会提出并组织实施，由上海市经济和信息化委员会、中共上海市委网络安全和信息化委员会办公室归口。

### （二）编制背景

区块链是新一代信息技术的重要组成部分，是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，通过数据透明、不易篡改、可追溯，有望解决网络空间的信任和安全问题，推动互联网从传递信息向传递价值变革，重构信息产业体系。

目前，区块链技术和应用正处于快速发展期。国际上，主要国际组织ITU、ISO、IEEE共发布区块链/分布式账本技术相关标准23项，其中22项在2020年正式发布，聚焦于技术和数据基础、安全和隐私两部分。然而，我国这方面的标准化进展相对滞后，2020年实现了行业标准零的突破，但还没有国家标准。其中，区块链安全标准更是匮乏。

为贯彻落实习近平总书记在中央政治局第十八次集体学习时的重要讲话精神，加强对区块链技术的引导和规范，加强对区块链安全风险的研究和分析，探索建立适应区块链技术机制的安全保障体系，推动上海地区区块链安全有序发展，推动区块链标准特别是区块链安全相关标准的发展，制定本标准。

### （三）主要起草单位和工作组成员

本标准由上海市信息安全测评认证中心（以下简称“上海测评中心”）主要牵头起草，苏州同济区块链研究院有限公司、上海七印信息科技有限公司、上海

墨珩网络科技有限公司、电信科学技术第一研究所有限公司等单位共同参与该标准的起草工作。

工作组成员包括：陈清明、顾敏、罗新辉、徐御、金铭彦、徐鑫、陈序、甘露、王一帆、阚肖庆、马小峰、吴鹏、陈小虎等。

#### **（四）主要工作过程**

**前期研究阶段：**参与区块链团标T/SSIA 0002-2018《区块链技术安全通用规范》，为本标准的编制打下了基础。

1、2018年3月——2018年12月，上海测评中心作为T/SSIA 0002-2018《区块链技术安全通用规范》团标编制项目的牵头单位，完成项目编制工作。

**标准立项阶段：**建立和完善标准文本架构，组织内部研讨和专家评审会，修改完善标准草案，完成标准立项。

2、2018年12月——2019年2月，开展标准文本架构研讨，组织召开3次线下内部技术研讨会，与标准起草单位共同完成标准草案，并根据专家、企业以及主管部门的综合意见进行修改。

3、2019年4月，在上海市市场监管局标准技术管理处组织的立项会上立项。

**标准研制阶段：**组织内部研讨和专家评审会，重点调整优化内容结构，形成征求意见稿。

4、2019年4月——2020年9月，对标准草案进行讨论和完善，并组织标准参编单位就区块链的体系架构、面临的安全风险以及安全要求等关键问题展开研讨，于2020年9月形成标准征求意见稿。

**标准征求意见阶段：**先后在网信上海公众号以及上海市市场监督管理局官网上面向社会公开征求意见。

5、2020年9月——2020年10月，根据上海市地方标准制修订要求，《区块链技术安全通用规范（征求意见稿）》在网信上海公众号上公开征求意见，公示1个月，截至10月9日，共收到3家单位16条反馈意见。

6、根据反馈意见，测评中心组织参编单位开展一次线下研讨会，对标准内容进行修改完善。

7、2020年11月17日，《区块链技术安全通用规范（征求意见稿）》在上海市市场监督管理局上公开征求意见，公示1个月。截至12月16日，没有收到反馈意见。

**标准送审阶段：**组织专家评审并报主管部门审查，完善标准条目的完备性和科学性形成标准送审稿，根据审定会专家意见，将标准名称修改为《区块链技术安全通用要求》。

8、2021年2月2日，上海市信安标委（地标委）组织业内专家召开标准技术审查会。

9、2021年2月——2021年3月，根据技术审查会专家意见，修改完善标准。

10、2021年3月，参加上海市市场监督管理局组织的专家审定会，根据专家意见修改完善标准，特别的，将标准名称修改为《区块链技术安全通用要求》，理由是通用规范的范围太大，通用要求与标准内容更加贴近。

**标准报批阶段：**根据专家意见，对标国内外区块链标准，形成标准报批稿。

## 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

### （一）标准编制原则

《区块链技术安全通用要求》的编制遵循以下原则：

- 1、先进性：标准反映当今区块链技术最新的发展态势；
- 2、开放性：标准的编制、评审与使用具有开放性；
- 3、适应性：标准结合我国以及上海市区块链发展实际；
- 4、简明性：标准易于理解、实现和应用；
- 5、中立性：公正、中立，不与任何利益攸关方发生关联；
- 6、一致性：术语与国内外标准所用术语最大程度保持一致。

### （二）标准主要内容的论据

本标准编写的格式遵从GB/T 1.1—2020的要求，技术和内容主要依据信息安全系统相关标准以及区块链相关标准，包括：

GB/T 22239 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语 标准

### （三）标准解决的主要问题

本标准充分考虑区块链的技术特点和发展态势，从安全角度出发解决如下问题：

- 1、聚焦区块链自身的技术通用性安全，重点分析区块链核心机制内在安全缺陷以及部署应用过程中可能引发的安全风险；
- 2、通过研究和分析区块链安全风险，提出适应区块链技术机制的安全要求；
- 3、解决基于区块链技术的产品或应用的安全设计、开发、测试、维护环节缺乏技术依据的问题。

此外，依据本标准，还可以为主管监管部门开展区块链信息服务以及内容安全监管提供技术参考。

### （四）标准的主要内容

为了便于分析，结合最佳实践和已知区块链风险分布情况，本标准提出区块链技术的三层技术架构：基础设施层、协议层以及扩展层。基于三层技术架构，本标准聚焦于区块链自身的技术通用性安全，重点分析区块链核心机制内在安全缺陷以及部署应用过程中可能引发的安全风险。针对各个层面存在的、潜在的安全风险，本标准逐层提出了安全要求。附录A和附录B分别给出了协议层安全措施举例和扩展层安全措施举例。

本标准总共7章。第一章到第四章分别是范围、规范性引用文件、术语和定义以及缩略语。第五章是区块链技术架构，第六章是安全风险，第七章是安全要求，附录A是协议层安全措施举例，附录B是扩展层安全措施举例。

## 三、主要实验（或验证）情况分析

2019年以来，上海市信息安全测评认证中心积极开展区块链技术安全测评，已完成蚂蚁区块链科技（上海）有限公司、上海华瑞银行股份有限公司、中远海运科技股份有限公司、上海富友支付服务股份有限公司、上海华钦信息科技股份有限公司、复旦大学、上海欧冶金融信息服务股份有限公司等多个单位的区块链测评，积累了较为丰富的区块链测评经验。

在某区块链应用项目测评中，测评团队按照本标准（征求意见稿）条款制定了安全测评方案，通过技术验证、配置核查、渗透测试等方法，共发现各类安全问题40个。测评项总体符合率为55.1%，部分符合率为11.2%，不符合率为33.7%，区块链技术安全风险主要集中在共识机制、智能合约、接口等方面。通过分析安全测评发现的区块链安全风险，以及结合区块链应用项目建设单位采取各类安全措施的最佳实践，编制团队对本标准涉及的风险分析、安全要求等内容进行了不断优化。

开展区块链安全测评既在实践中检验了标准的合理性，也为标准编制提供了丰富的案例，在试用过程中反馈的意见、建议为标准的编制奠定了良好基础。

#### 四、知识产权情况说明

标准的技术内容不涉及专利。

#### 五、产业化情况、推广应用论证和预期达到的经济效果

区块链作为一项重要的新兴技术，在推动数字经济创新发展方面潜力巨大。本标准有助于建立区块链安全保障体系，确保区块链安全有序发展，推动区块链与实体经济深度融合，从而有力支撑上海城市数字化转型。

本标准发布后，计划用于区块链产品或应用开发企业开展区块链技术安全风险评估，以及据此开展的安全设计、安全加固、安全配置等，也适用于第三方评估机构开展区块链产品或应用的技术安全评估。同时，本标准也可用于有关部门开展区块链应用的安全监督检查，有助于把依法治网落实到区块链管理中，推动区块链安全有序发展。

#### 六、采用国内外标准和国内外先进标准情况

ITU-T Q14/SG17 已经开展区块链技术和应用场景安全研究，覆盖安全威胁、安全架构、安全保障、安全服务等维度，ITU-T Q17/SG13在研的区块链服务标准Y.BaaS-reqts旨在为云计算环境下的区块链服务提供功能需求，ITU-T Q8/SG17从安全角度开展区块链服务安全指南X.BaaSsec的研究，聚焦区块链服务的安全性。

目前，全国信息安全标准化组织（TC260）已开展区块链安全标准体系、区块链安全参考架构等相关研究，聚焦于区块链技术架构本身在设计、实现或实施方面的安全缺陷，重点解决顶层区块链安全体系架构构建的问题，提出区块链安全架构、关键安全组件及其安全能力要求等。在行业标准方面，通信行业从区块链应用、区块链产品和区块链基础设施等不同维度，构建总体和细化的区块链安全应用体系；金融行业已发布金融分布式账本技术安全规范，针对金融行业从事分布式账本系统建设或服务运营的机构，规定了应遵循的安全体系。

本标准编制过程中，广泛参考了国内外的相关区块链安全标准和规范，紧跟全国信息安全标准化组织（TC260）“聚焦于区块链技术架构本身在设计、实现或实施方面的安全缺陷，重点解决顶层区块链安全体系架构构建的问题”的研究思路。与YD/T 3747-2020《区块链技术架构安全要求》相同的是，本标准也采用三层区块链技术架构，但每个层面的具体划分和安全要求则有较大区别，本标准技术架构的划分是基于区块链技术的安全风险分布以及区块链项目测评实践，符合区块链安全发展态势和应用实际。本标准所提出的三层架构中，基础设施层将传统网络安全与区块链安全联系起来，包括存储、网络以及计算三个方面，基础设施层的安全要求借鉴引用GB/T 22239相关安全要求。协议层聚焦区块链核心机制，包含区块链技术的几大关键机制：共识机制、密码学机制、时序机制以及组网机制，协议层向下衔接基础设施层，向上衔接扩展层，为扩展层提供相应功能的支持服务。扩展层包括智能合约和服务与访问两部分，扩展层通过调用协议层功能组件，可以提供多元化的服务和访问。结合上海测评中心在多个区块链项目中的测评实践，本标准在分析总结区块链安全风险的基础上提出协议层和扩展层的安全要求。

本标准基于安全架构给出的风险分析和安全要求，对指导基于区块链技术的产品或应用的安全设计、开发、测试及维护具有重要意义。此外，本标准紧密结合网络安全发展现状，在协议层引入个人信息保护，在扩展层引入内容安全，这些内容的引入可为上海市有关部门开展区块链信息服务以及内容安全监管提供参考。因此，本标准项目的推进，对于促进我国的区块链安全标准化工作，展现上海市在区块链安全领域先行先试的先进地位，具有十分重要的意义。

## 七、与现行相关法律、法规、规章及相关标准的协调性

本标准与现行《网络安全法》、《区块链信息服务管理规定》、《密码法》等法律、法规、规章相协调配套。

本标准与现行相关标准无冲突和矛盾。

## 八、重大分歧意见的处理经过和依据

无

## 九、标准性质的建议

建议本标准作为上海市地方标准发布实施。

## 十、实施地方标准的要求和措施建议

为使标准更好地发挥技术指导作用，提高区块链系统的安全能力，建议做好宣传培训，使上海从事区块链设计、开发、维护和使用等工作的各单位掌握标准的各项技术安全要求，使安全标准的应用真正落到实处。同时，对《区块链技术安全通用要求》地方标准执行情况进行跟踪调查，及时发现标准中存在的问题，不断修订完善。

## 十一、替代或废止现行相关标准的建议

无。

## 十二、其它应予以说明的事项

无。

上海市地方标准《区块链技术安全通用要求》编制组

2021年8月16日