ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 42570—2023

# 信息安全技术　区块链技术安全框架

**Information security technology—Security framework for blockchain technology**

2023-05-23 发布　　2023-12-01 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

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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：清华大学、中国人民银行数字货币研究所、中国电子技术标准化研究院、国家信息技术安全研究中心、蚂蚁科技集团股份有限公司、京东科技信息技术有限公司、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、矩阵元技术(深圳)有限公司、深圳市腾讯计算机系统有限公司、浙江大学、上海交通大学。

本文件主要起草人：王小云、穆长春、狄刚、贾珂婷、郭晓雷、王海军、张爽、王海棠、张韧、王宗岳、郁昱、魏普文、段斯斯、潘国振、王博、苏年乐、金涛、龚自洪、昌文婷、荆博、张海滨、何超、王海龙、邱鹏程、陈宇、王安宇、陈平、郭山清、张国艳、任奎、张宇光、孙晓丽、刘健、秦岭月、李克鹏。

# 信息安全技术　区块链技术安全框架

## 1　范围

本文件给出了区块链技术安全框架，该框架包括区块链密码支撑、区块链安全功能组件、区块链安全管理运行和区块链角色安全职责等部分。

本文件适用于指导区块链业务提供者在区块链设计、开发、部署、管理和运维的过程中进行整体规划和安全框架设计，也可为开展区块链安全评估提供参考。

## 2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20518　信息安全技术　公钥基础设施 数字证书格式

GB/T 21053　信息安全技术　公钥基础设施 PKI 系统安全等级保护技术要求

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

GB/T 25069　信息安全技术　术语

GB/T 30998　信息技术　软件安全保障规范

GB/T 35273—2020　信息安全技术　个人信息安全规范

GB/T 37092—2018　信息安全技术　密码模块安全要求

GB/T 39786—2021　信息安全技术　信息系统密码应用基本要求

GM/T 0005　随机性检测规范

## 3　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

**区块　block**

一种由一系列信息单元组成的基本数据结构。

[来源：ISO 22739：2020，3.2，有修改]

3.2

**区块链　blockchain**

将区块顺序相连，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

[来源：ISO 22739：2020，3.6，有修改]

3.3

**节点　node**

具有特定功能的可独立运行的区块链组件。