



中华人民共和国公共安全行业标准

GA/T 1390.9—2025

信息安全技术 网络安全等级保护基本要求 第9部分：区块链安全扩展要求

Information security technology—Baseline for classified protection of
cybersecurity—Part 9: Extended requirements for blockchain security

2025-10-13发布

2026-02-01实施

中华人民共和国公安部 发布

目次

前言Ⅲ

引言Ⅳ

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 第一级安全扩展要求3

6 第二级安全扩展要求3

7 第三级安全扩展要求5

8 第四级安全扩展要求7

9 第五级安全扩展要求9

附录 A(资料性) 区块链安全扩展要求的选择和使用10

参考文献14

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。

本文件是 GA/T 1390《信息安全技术 网络安全等级保护基本要求》的第 9 部分。GA/T 1390 已经发布了以下部分：

- 第 2 部分：云计算安全扩展要求；
- 第 3 部分：移动互联安全扩展要求；
- 第 5 部分：工业控制系统安全扩展要求；
- 第 6 部分：边缘计算安全扩展要求；
- 第 7 部分：大数据系统安全扩展要求；
- 第 8 部分：IPv6 网络安全扩展要求；
- 第 9 部分：区块链安全扩展要求。

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。

本文件由公安部网络安全保卫局提出。

本文件由公安部信息系统安全标准化技术委员会归口。

本文件起草单位：公安部第三研究所、公安部网络安全保卫局、公安部第一研究所、国家计算机病毒应急处理中心、中国移动通信有限公司研究院、华为技术有限公司、腾讯云计算(北京)有限责任公司、长春吉大正元信息技术股份有限公司。

本文件主要起草人：陶源、李末岩、王李乐、游志勇、任娟娟、陈建民、李秋香、赵大鹏、任兰芳、陈雪、黄敏、薛腾飞、李克鹏、韩璇、刘伟康。

引 言

GA/T 1390《信息安全技术 网络安全等级保护基本要求》旨在提出不同网络安全保护等级的基线安全要求,指导等级保护对象的安全建设和监督管理。GA/T 1390 拟由以下部分组成。

- 第 1 部分:安全通用要求。旨在提出适用于所有网络安全等级保护对象的安全基线要求。
- 第 2 部分:云计算安全扩展要求。旨在提出适用于云计算平台/系统的安全扩展要求。
- 第 3 部分:移动互联安全扩展要求。旨在提出适用于采用移动互联技术的等级保护对象的安全扩展要求。
- 第 4 部分:物联网安全扩展要求。旨在提出适用于物联网的安全扩展要求。
- 第 5 部分:工业控制系统安全扩展要求。旨在提出适用于工业控制系统的安全扩展要求。
- 第 6 部分:边缘计算安全扩展要求。旨在提出适用于采用边缘计算技术的等级保护对象的安全扩展要求。
- 第 7 部分:大数据系统安全扩展要求。旨在提出适用于采用大数据技术的等级保护对象的安全扩展要求。
- 第 8 部分:IPv6 网络安全扩展要求。旨在提出适用于 IPv6 等级保护对象的安全扩展要求。
- 第 9 部分:区块链安全扩展要求。旨在提出适用于区块链等级保护对象的安全扩展要求。
- 第 10 部分:生成式人工智能安全扩展要求。旨在提出适用于生成式人工智能等级保护对象的安全扩展要求。
- 第 11 部分:低空智联网安全扩展要求。旨在提出适用于低空智联网等级保护对象的安全扩展要求。
- 第 12 部分:智能车联网安全扩展要求。旨在提出适用于智能车联网等级保护对象的安全扩展要求。

信息安全技术 网络安全等级保护基本要求 第9部分：区块链安全扩展要求

1 范围

本文件规定了区块链等级保护对象的网络安全等级保护第一级到第四级的安全扩展要求。
本文件适用于联盟链和私有链的安全建设和监督管理。

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 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 22240 信息安全技术 网络安全等级保护定级指南
- GB/T 37092—2018 信息安全技术 密码模块安全要求
- GB/T 39786 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 22239、GB/T 22240 和 GB/T 39786 界定的以及下列术语和定义适用于本文件。

3.1

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:GB/T 42570—2023,3.2]

3.2

私有链 private blockchain

由单个用户授权的区块链点可接入,接入节点可按规则参与共识和读写数据的区块链部署模型。

[来源:GM/T 0111—2021,3.9,有修改]

3.3

联盟链 consortium blockchain

对特定组织团体开放的区块链,节点通过管理员或管理机构授权后方可加入区块链,所有共识节点的地址互相知晓并可互相通信的区块链。

[来源:GB/T 42570—2023,3.11]

3.4

区块链节点 blockchain node

具有共识机制、智能合约等特定功能的区块链组件,可独立运行的单元。

[来源:GB/T 42570—2023,3.3,有修改]

3.5

区块链平台 **blockchain platform**

基于区块链技术,连接多个区块链节点并提供其上智能合约、共识机制等服务的软硬件集合。

3.6

区块链应用 **blockchain application**

使用区块链平台服务构建的业务应用系统。

3.7

交易 **transaction**

工作流程的最小操作单元。

[来源:GB/T 42570—2023,3.5]

3.8

用户 **user**

参与产生区块链交易数据的个人、组织或进程。

[来源:GB/T 42570—2023,3.6]

3.9

共识机制 **consensus mechanism**

实现不同区块链节点之间建立信任、达成一致的机制。

[来源:GB/T 42570—2023,3.7,有修改]

3.10

智能合约 **smart contract**

由用户部署在区块链中,且执行结果记录于区块链的计算机程序。

[来源:GB/T 42570—2023,3.12]

3.11

分布式账本 **distributed ledger**

在一组分布式账本技术节点之间共享并使用共识机制同步的账本。

[来源:GB/T 43573—2023,3.23,有修改]

4 概述

区块链等级保护对象包括区块链平台和区块链应用。区块链等级保护对象在区跨链平台和区块链应用面临着与其他等级保护对象相似的安全风险,并且区块链等级保护对象的智能合约和共识机制等面临着新的安全风险。区块链平台及区块链应用的典型架构如图 1 所示。

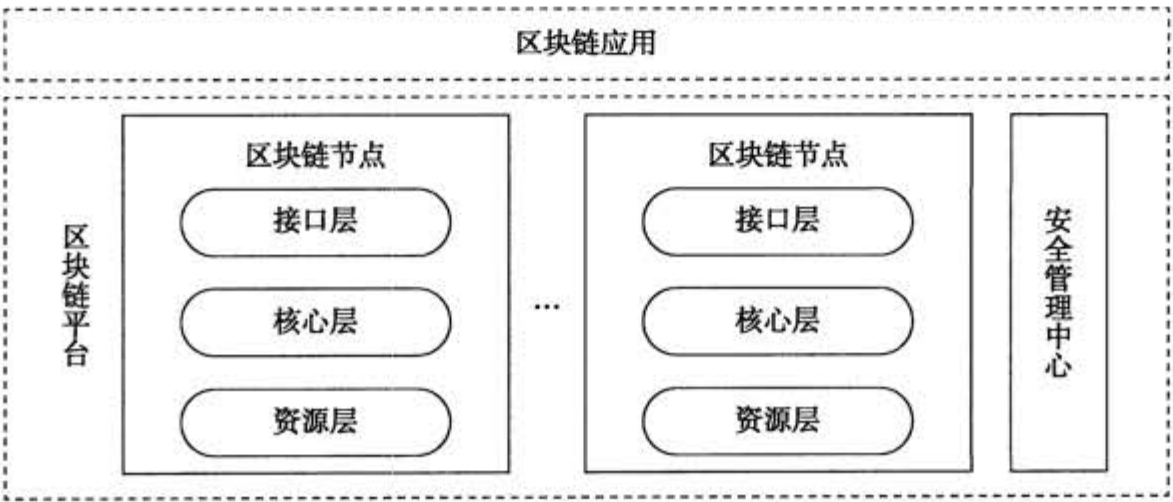


图 1 区块链平台及区块链应用的典型架构

在图 1 中,区块链节点可抽象为资源层、核心层和接口层。在区块链节点中,资源层提供区块链运行所需要的物理服务器、虚拟机以及容器等基础资源;核心层包括共识机制、智能合约等多种区块链核心功能,可能运行共识机制和智能合约的一种或多种;接口层对区块链应用屏蔽底层细节,形成高效易用的、标准化的开发接口,以软件开发工具包、远程过程调用、表述性状态转移等方式提供服务。区块链应用是基于区块链平台提供服务的业务应用系统。典型的区块链应用包括存证、溯源和对账等应用。

区块链等级保护对象可以是区块链平台和区块链应用的组合,也可以单独是区块链平台或区块链应用。区块链安全扩展要求项的选择和使用见附录 A。

5 第一级安全扩展要求

5.1 安全物理环境

区块链平台应位于中国境内。

5.2 安全通信网络

安全通信网络的网络架构应满足以下要求:

- a) 区块链应用不能使用低于其安全保护等级的区块链平台服务;
- b) 离线区块链节点重新加入区块链平台后,能进行数据同步。

5.3 安全计算环境

5.3.1 身份鉴别

区块链平台应提供白名单等身份鉴别机制进行节点接入限制,防止未经鉴别节点加入区块链平台。

5.3.2 数据完整性

交易与分布式账本应在多数区块链节点拥有完整的数据记录,实现各区块链节点数据的一致性。

6 第二级安全扩展要求

6.1 安全物理环境

区块链平台应位于中国境内。

6.2 安全通信网络

安全通信网络的网络架构应满足以下要求:

- a) 区块链应用不能使用低于其安全保护等级的区块链平台服务;
- b) 离线区块链节点重新加入区块链平台后,能进行数据同步;
- c) 区块链节点正常重启或从异常场景恢复后,能参与共识和同步数据,实现区块链节点数据一致;
- d) 能动态增删区块链节点,提供动态扩容能力,且不影响区块链应用。

6.3 安全计算环境

6.3.1 身份鉴别

身份鉴别应满足以下要求:

- a) 区块链平台提供白名单等身份鉴别机制进行节点接入限制,防止未经鉴别节点加入区块链

平台；

- b) 对管理区块链平台的管理人员进行身份鉴别。

6.3.2 访问控制

访问控制应满足以下要求：

- a) 具备智能合约授权访问控制能力，限制不同类型用户对区块链平台资源的读取、写入等访问权限；
- b) 具备有效的请求失败识别和处理能力，例如结束会话、限制非法访问次数和超时自动退出等功能；
- c) 对访问区块链平台智能合约的用户进行访问授权。

6.3.3 安全审计

对区块链平台智能合约的部署和运行进行安全性审计。

6.3.4 智能合约安全

智能合约安全应满足以下要求：

- a) 对区块链平台用户提供智能合约安全开发规范，明确智能合约在运行安全、接口安全、安全配置等方面的开发安全要求；
- b) 建立区块链平台智能合约的仲裁响应机制，能在仲裁后执行智能合约冻结和恢复等相关措施，并保留相应的记录；
- c) 区块链节点实现合约调用与执行安全，能安全处理异常调用，具有检测恶意代码和安全漏洞的能力，并定期进行检测，及时修复、更新。

6.3.5 共识机制安全

应披露区块链平台的共识机制、同步网络模型，容错条件以及适用场景。

6.3.6 数据完整性

数据完整性应满足以下要求：

- a) 交易与分布式账本在多数区块链节点拥有完整的数据记录，实现各区块链节点数据的一致性；
- b) 采用校验技术或密码技术实现交易数据与分布式账本数据在各个区块链节点的完整性。

6.3.7 数据保密性

应使用密码技术实现交易数据与分布式账本数据中敏感个人信息的安全存储和安全传输。

6.4 安全运维管理

6.4.1 密码管理

采用的密码产品应满足 GB/T 37092—2018 一级及以上安全要求。

6.4.2 密钥管理

密钥进行生命周期管理，不为永久有效，到达一定的时间周期后需要更换。

6.4.3 区块链运维环境管理

区块链运维环境管理应满足以下要求：

- a) 区块链节点具有版本后向兼容性,区块链节点升级后仍支持旧版本的数据；
- b) 区块链管理平台的运维地点位于中国境内。

7 第三级安全扩展要求

7.1 安全物理环境

区块链平台应位于中国境内。

7.2 安全通信网络

安全通信网络的网络架构应满足以下要求：

- a) 区块链应用不能使用低于其安全保护等级的区块链平台服务；
- b) 离线区块链节点重新加入区块链平台后,能进行数据同步；
- c) 区块链节点正常重启或从异常场景恢复后,能参与共识和同步数据,实现区块链节点数据一致；
- d) 能动态增删区块链节点,提供动态扩容能力,且不影响区块链应用；
- e) 区块链节点的通信进行双向鉴别。

7.3 安全计算环境

7.3.1 身份鉴别

身份鉴别应满足以下要求：

- a) 区块链平台通过身份鉴别机制和安全访问措施进行节点接入限制,防止未经鉴别节点加入区块链平台；
- b) 对管理区块链平台的管理人员进行身份鉴别。

7.3.2 访问控制

访问控制应满足以下要求：

- a) 具备有效的访问控制策略,限制不同类型用户对区块链平台资源的读取、写入等访问权限；
- b) 具备有效的请求失败识别和处理能力,例如结束会话、限制非法访问次数和超时自动退出等功能；
- c) 对访问区块链平台智能合约的用户进行访问授权；
- d) 依照最小必要原则向区块链平台和区块链应用的用户开放敏感数据访问授权,并且需要数据所有者授权；
- e) 对区块链应用中的分布式账本数据和状态数据的查询和操作采用访问控制技术进行限制,防止未授权读取和篡改。

7.3.3 安全审计

安全审计应满足以下要求：

- a) 对区块链平台智能合约的部署和运行进行安全审计；
- b) 对区块链应用的链上数据的更新、删除、所属权变更等操作进行审计；
- c) 区块链平台对区块链应用的数据操作可被区块链应用的用户审计。

7.3.4 智能合约安全

智能合约安全应满足以下要求：

- a) 对区块链平台用户提供智能合约安全开发规范,明确智能合约在运行安全、接口安全、安全配置等方面的开发安全要求;
- b) 建立区块链平台智能合约的仲裁响应机制,能在仲裁后执行智能合约冻结和恢复等相关措施,并保留相应的记录;
- c) 区块链节点实现合约调用与执行安全,能安全处理异常调用,具有检测恶意代码和安全漏洞的能力,并定期进行检测,及时修复、更新;
- d) 对区块链平台的智能合约进行安全检测,包括智能合约基线安全检测、框架性安全检测、源代码安全检测等,并将检测结果情况告知用户;
- e) 智能合约之间调用进行调用权限校验和限制。

7.3.5 共识机制安全

共识机制安全应满足以下要求：

- a) 披露区块链平台的共识机制、同步网络模型,容错条件以及适用场景;
- b) 区块链平台的共识机制支持区块链节点动态扩容、扩容;
- c) 区块链平台的共识机制具有容错性及一致性,具备防重放攻击的能力。

7.3.6 数据完整性

数据完整性应满足以下要求：

- a) 交易与分布式账本在多数区块链节点拥有完整的数据记录,实现各区块链节点数据的一致性;
- b) 采用密码技术实现交易数据与分布式账本数据在各个区块链节点的完整性。

7.3.7 数据保密性

数据保密性应满足以下要求：

- a) 使用密码技术实现交易数据与分布式账本数据中敏感个人信息的安全存储;
- b) 只有在数据所有者授权下,区块链平台运营者或第三方才具有区块链应用的数据管理权限。

7.4 安全管理中心

安全管理中心的集中管控应满足以下要求：

- a) 对区块链平台的业务运行状况进行集中监测,包括已上链交易数量、待处理交易数量以及合约数量等;
- b) 当监测的业务资源超出设定的范围时进行告警。

7.5 安全运维管理

7.5.1 密码管理

采用的密码产品应满足 GB/T 37092—2018 二级及以上安全要求。

7.5.2 密钥管理

密钥管理应满足以下要求：

- a) 区块链平台和应用中的身份鉴别密钥、数据加密密钥等,使用通过商用密码检测认证的密码设

备或模块对密钥的生成、存储、分发、导入与导出、使用、备份与恢复、归档、销毁等环节实现安全管理；

- b) 对区块链节点之间的通信数据加密,并对区块链节点上存储数据加密,通过商用密码检测认证的密码设备或模块将私钥妥善保存；
- c) 对密钥进行生命周期管理,不为永久有效,到达一定的时间周期后需要更换。

7.5.3 区块链运维环境管理

区块链运维环境管理应满足以下要求：

- a) 区块链节点具有版本后向兼容性,区块链节点升级后仍支持旧版本的数据；
- b) 区块链管理平台的运维地点位于中国境内。

8 第四级安全扩展要求

8.1 安全物理环境

区块链平台应位于中国境内。

8.2 安全通信网络

安全通信网络的网络架构应满足以下要求：

- a) 区块链应用不能使用低于其安全保护等级的区块链平台服务；
- b) 离线区块链节点重新加入区块链平台后,能进行数据同步；
- c) 区块链节点正常重启或从异常场景恢复后,能参与共识和同步数据,实现区块链节点数据一致；
- d) 能动态增删区块链节点,提供动态扩容能力,且不影响区块链应用；
- e) 区块链节点的通信进行双向鉴别。

8.3 安全计算环境

8.3.1 身份鉴别

身份鉴别应满足以下要求：

- a) 区块链平台通过身份鉴别机制和安全管控措施进行节点接入限制,防止未经鉴别节点加入区块链平台；
- b) 对管理区块链平台的管理人员进行身份鉴别。

8.3.2 访问控制

访问控制应满足以下要求：

- a) 具备有效的访问控制策略,限制不同类型用户对区块链平台资源的读取、写入等访问权限；
- b) 具备有效的请求失败识别和处理能力,例如结束会话、限制非法访问次数和超时自动退出等功能；
- c) 对访问区块链平台智能合约的用户进行访问授权；
- d) 依照最小必要原则向区块链平台和区块链应用的用户开放敏感数据访问授权,并且需要数据所有者授权；
- e) 对区块链应用中的分布式账本数据和状态数据的查询和操作采用访问控制技术进行限制,防止未授权读取和篡改。

8.3.3 安全审计

安全审计应满足以下要求：

- a) 对区块链平台智能合约的部署和运行进行安全审计；
- b) 对区块链应用的链上数据的更新、删除、所属权变更等操作进行审计；
- c) 区块链平台对区块链应用的数据操作可被区块链应用的用户审计。

8.3.4 智能合约安全

智能合约安全应满足以下要求：

- a) 对区块链平台用户提供智能合约安全开发规范,明确智能合约在运行安全、接口安全、安全配置等方面的开发安全要求；
- b) 建立区块链平台智能合约的仲裁响应机制,可在仲裁后执行智能合约冻结和恢复等相关措施,并保留相应的记录；
- c) 区块链节点实现合约调用与执行安全,可以安全处理异常调用,具有检测恶意代码和安全漏洞的能力,并定期进行检测,及时修复、更新；
- d) 对区块链平台的智能合约进行安全检测,包括智能合约基线安全检测、框架性安全检测、源代码安全检测等,并将检测结果情况告知用户；
- e) 智能合约之间调用进行调用权限校验和限制。

8.3.5 共识机制安全

共识机制安全应满足以下要求：

- a) 披露区块链平台的共识机制、同步网络模型,容错条件以及适用场景；
- b) 区块链平台的共识机制支持区块链节点动态扩容、扩容；
- c) 区块链平台的共识机制具有容错性及一致性,具备防重放攻击的能力。

8.3.6 数据完整性

数据完整性应满足以下要求：

- a) 交易与分布式账本在多数区块链节点拥有完整的数据记录,实现各区块链节点数据的一致性；
- b) 采用密码技术实现交易数据与分布式账本数据在各个区块链节点的完整性。

8.3.7 数据保密性

数据保密性应满足以下要求：

- a) 使用密码技术实现交易数据与分布式账本数据中个人隐私信息的安全存储；
- b) 只有在数据所有者授权下,区块链平台运营者或第三方才具有区块链应用的数据管理权限。

8.4 安全管理中心

安全管理中心的集中管控应满足以下要求：

- a) 对区块链平台的业务运行状况进行集中监测,包括已上链交易数量、待处理交易数量以及合约数量等；
- b) 当监测的业务资源超出设定的范围时进行告警。

8.5 安全运维管理

8.5.1 密码管理

采用的密码产品应满足 GB/T 37092—2018 三级及以上安全要求。

8.5.2 密钥管理

密钥管理应满足以下要求：

- a) 区块链平台和应用中的身份鉴别密钥、数据加密密钥等,使用通过商用密码检测认证的密码设备或模块对密钥的生成、存储、分发、导入与导出、使用、备份与恢复、归档、销毁等环节实现安全管理；
- b) 对区块链节点之间的通信数据加密,并对区块链节点上存储数据加密,通过商用密码检测认证的密码设备或模块将私钥妥善保存；
- c) 对密钥进行生命周期管理,不为永久有效,到达一定的时间周期后需要更换。

8.5.3 区块链运维环境管理

区块链运维环境管理应满足以下要求：

- a) 区块链节点具有版本后向兼容性,区块链节点升级后仍支持旧版本的数据；
- b) 区块链管理平台的运维地点位于中国境内。

9 第五级安全扩展要求

略。

附录 A

(资料性)

区块链安全扩展要求的选择和使用

区块链安全扩展要求项与区块链等级保护对象关系见表 A.1~表 A.4。

表 A.1 第一级区块链安全扩展要求项与区块链等级保护对象对照表

安全类	控制点	要求项	区块链平台	区块链应用
安全物理环境	—	5.1	★	—
安全通信网络	—	5.2 a)	★	★
		5.2 b)	★	—
安全计算环境	身份鉴别	5.3.1	★	—
	访问控制	5.3.2	★	—
注：“★”代表要求项与等级保护对象匹配，“—”代表要求项与等级保护对象不匹配。				

表 A.2 第二级区块链安全扩展要求项与区块链等级保护对象对照表

安全类	控制点	要求项	区块链平台	区块链应用
安全物理环境	—	6.1	★	—
安全通信网络	—	6.2 a)	★	★
		6.2 b)	★	—
		6.2 c)	★	—
		6.2 d)	★	★
安全计算环境	身份鉴别	6.3.1 a)	★	—
		6.3.1 b)	★	—
	访问控制	6.3.2 a)	★	—
		6.3.2 b)	★	—
		6.3.2 c)	★	—
	安全审计	6.3.3	★	—
	智能合约安全	6.3.4 a)	★	—
		6.3.4 b)	★	—
		6.3.4 c)	★	—
	共识机制安全	6.3.5	★	—
	数据完整性	6.3.6 a)	★	—
		6.3.6 b)	★	—
	数据保密性	6.3.7	★	—

表 A.2 第二级区块链安全扩展要求项与区块链等级保护对象对照表（续）

安全类	控制点	要求项	区块链平台	区块链应用
安全运维管理	密码管理	6.4.1	★	—
	密钥管理	6.4.2	★	★
	区块链运维环境管理	6.4.3 a)	★	—
		6.4.3 b)	★	—
注：“★”代表要求项与等级保护对象匹配，“—”代表要求项与等级保护对象不匹配。				

表 A.3 第三级区块链安全扩展要求项与区块链等级保护对象对照表

安全类	控制点	要求项	区块链平台	区块链应用
安全物理环境	—	7.1	★	—
安全通信网络	—	7.2 a)	★	★
		7.2 b)	★	—
		7.2 c)	★	—
		7.2 d)	★	★
		7.2 e)	★	—
安全计算环境	身份鉴别	7.3.1 a)	★	—
		7.3.1 b)	★	—
	访问控制	7.3.2 a)	★	—
		7.3.2 b)	★	★
		7.3.2 c)	★	★
		7.3.2 d)	★	★
		7.3.2 e)	★	★
	安全审计	7.3.3 a)	★	—
		7.3.3 b)	★	★
		7.3.3 c)	★	★
	智能合约安全	7.3.4 a)	★	—
		7.3.4 b)	★	—
		7.3.4 c)	★	—
		7.3.4 d)	★	—
		7.3.4 e)	★	—
	共识机制安全	7.3.5 a)	★	—
		7.3.5 b)	★	—
		7.3.5 c)	★	—
	数据完整性	7.3.6 a)	★	—

表 A.3 第三级区块链安全扩展要求项与区块链等级保护对象对照表（续）

安全类	控制点	要求项	区块链平台	区块链应用
安全计算环境	数据完整性	7.3.6 b)	★	—
	数据保密性	7.3.7 a)	★	—
		7.3.7 b)	★	—
安全管理中心	—	7.4 a)	★	—
		7.4 b)	★	—
安全运维管理	密码管理	7.5.1	★	★
	密钥管理	7.5.2 a)	★	★
		7.5.2 b)	★	—
		7.5.2 c)	★	★
	区块链运维环境管理	7.5.3 a)	★	—
		7.5.3 b)	★	—
注：“★”代表要求项与等级保护对象匹配，“—”代表要求项与等级保护对象不匹配。				

表 A.4 第四级区块链安全扩展要求项与区块链等级保护对象对照表

安全类	控制点	要求项	区块链平台	区块链应用
安全物理环境	—	8.1	★	—
安全通信网络	—	8.2 a)	★	★
		8.2 b)	★	—
		8.2 c)	★	—
		8.2 d)	★	★
		8.2 e)	★	—
安全计算环境	身份鉴别	8.3.1 a)	★	—
		8.3.1 b)	★	—
	访问控制	8.3.2 a)	★	—
		8.3.2 b)	★	★
		8.3.2 c)	★	★
		8.3.2 d)	★	★
		8.3.2 e)	★	★
	安全审计	8.3.3 a)	★	—
		8.3.3 b)	★	★
		8.3.3 c)	★	★
	智能合约安全	8.3.4 a)	★	—
		8.3.4 b)	★	—

表 A.4 第四级区块链安全扩展要求项与区块链等级保护对象对照表（续）

安全类	控制点	要求项	区块链平台	区块链应用
安全计算环境	智能合约安全	8.3.4 c)	★	—
		8.3.4 d)	★	—
		8.3.4 e)	★	—
	共识机制安全	8.3.5 a)	★	—
		8.3.5 b)	★	—
		8.3.5 c)	★	—
	数据完整性	8.3.6 a)	★	—
		8.3.6 b)	★	—
	数据保密性	8.3.7 a)	★	—
		8.3.7 b)	★	—
安全管理中心	—	8.4 a)	★	—
		8.4 b)	★	—
安全运维管理	密码管理	8.5.1	★	★
	密钥管理	8.5.2 a)	★	★
		8.5.2 b)	★	—
		8.5.2 c)	★	★
	区块链运维环境管理	8.5.3 a)	★	—
		8.5.3 b)	★	—
注：“★”代表要求项与等级保护对象匹配，“—”代表要求项与等级保护对象不匹配。				

参 考 文 献

- [1] GB/T 42570—2023 信息安全技术 区块链技术安全框架
 - [2] GB/T 42571—2023 信息安全技术 区块链信息服务安全规范
 - [3] GB/T 42752—2023 区块链和分布式记账技术 参考架构
 - [4] GB/T 43575—2023 区块链和分布式记账技术 系统测试规范
 - [5] 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
 - [6] GB/T 43580—2023 区块链和分布式记账技术 存证通用服务指南
 - [7] GB/T 43582—2023 区块链和分布式记账技术 应用程序接口 中间件技术指南
 - [8] GM/T 0111—2021 区块链密码应用技术要求
 - [9] ITU-T F.751.14 Reference architecture for information tracing of renewable energy consumption based on distributed ledger technology
 - [10] ITU-T F.751.15 Assessment methods for distributed ledger technology (DLT) management service platforms
 - [11] ITU-T F.751.16 Reference framework for distributed ledger technology (DLT) management service platforms
 - [12] ISO/TC 307 Blockchain and distributed ledger technologies—Data flow models for blockchain and DLT use cases
 - [13] IEEE 3219—2023 Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things
-

中华人民共和国公共安全
行 业 标 准
信息安全技术 网络安全等级保护基本
要求 第9部分：区块链安全扩展要求
GA/T 1390.9—2025

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

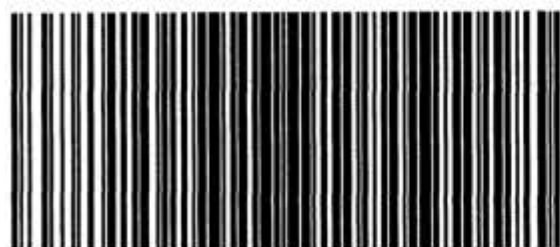
*

开本 880×1230 1/16 印张 1.5 字数 31 千字
2025年12月第1版 2025年12月第1次印刷

*

书号: 155066 • 2-39571 定价 43.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68510107



GA/T 1390.9-2025