

团 体 标 准

T/CESA 1221—2022

区块链 专用服务网络 基础设施总体要求

**Blockchain—Private service network—General requirements
for infrastructure**

2022-08-29 发布

2022-09-29 实施

中国电子工业标准化技术协会 发布

目 次

前言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 通用要求和总体框架	4
5.1 通用要求	4
5.2 总体框架	4
6 基础层	6
6.1 部署环境要求	6
6.2 硬件设备要求	6
6.3 基础软件要求	6
6.4 网络环境要求	7
7 支撑层	7
7.1 底层框架	7
7.2 密码算法	8
7.3 跨链机制	9
8 接入层	9
8.1 部署配置	9
8.2 交易鉴权	10
8.3 请求路由	10
8.4 事件通知	10
8.5 交易限流	10
8.6 负载均衡	10
8.7 监控报警	10
8.8 网关 SDK	10
9 应用层	10
9.1 应用发布	10
9.2 应用部署	11
9.3 应用参与	11
9.4 应用接入	11
9.5 应用升级	11
9.6 应用卸载	11
10 与外部节点的数据交换	11
10.1 数据交换	11

10.2 身份管理	11
10.3 通信安全	11
10.4 权限管理	11
11 运行维护	12
11.1 底层框架管理	12
11.2 节点网关管理	12
11.3 系统运行监控	12
11.4 备份与恢复	12
11.5 应急预案管理	12
12 安全体系	12
12.1 底层框架节点身份	12
12.2 底层框架通信安全	12
12.3 网关通信安全	13
12.4 应用接入身份	13
12.5 应用权限管理	13
12.6 用户身份管理	13
13 监管机制	13
13.1 监管内容	13
13.2 监管方式	13
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。

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。

本文件由国家信息中心提出。

本文件由中国电子工业标准化技术协会归口。

本文件起草单位:国家信息中心、中国移动通信集团设计院有限公司、中国银联股份有限公司、北京红枣科技有限公司、深圳前海微众银行股份有限公司、湖北省发展和改革委员会、重庆江北区大数据应用发展管理局、重庆市区块链数字经济产业园管委会、长春政务服务和数字化建设管理局、长春市信息中心、长沙市数据资源管理局、中国移动通信有限公司政企客户分公司、中国移动通信集团重庆有限公司、中国移动通信集团湖北有限公司、中国移动通信集团甘肃有限公司、中国移动通信集团浙江有限公司杭州分公司、中国移动通信集团宁夏有限公司、中国移动通信集团江苏有限公司、中国移动通信集团海南有限公司、中国移动通信集团河北有限公司、中国移动通信集团吉林有限公司、中国移动通信集团湖南有限公司长沙分公司、海南火链科技有限公司、中国雄安集团数字城市科技有限公司、苏州市相城区区块链科技有限公司、北京国信恒达智慧城市科技发展有限公司、易盾链动(重庆)数字科技有限公司、北京泰豪智能工程有限公司、北京百度网讯科技有限公司。

本文件主要起草人:单志广、高鹏、谭敏、何亦凡、许玉壮、邓伟平、李贺、代翔、郎晓夫、张高山、詹义、杨鹏、费光荣、魏飞、马晓军、刘国栋、张延强、陈栩、唐斯斯、马潮江、戴彧、王丹丹、闫晓丽、涂菲菲、朱华、倪宁宁、刘仲思、咸燕、范瑞彬、张开翔、吴芸、肖竞佳、石飞前、邓永俊、于本江、李欣、庄毅、王也、丁慧东、赵哲、柳羽辉、叶亭吟、罗斌、何青阳、张程、刘焱宇、吴波、饶毅、贾奋勇、张磊、张明明、王文生、屠宇飞、柳毅、朱智俊、童洲游、段立、吴东平、张峻岭、杨鹏、孙思远、许慧莹、邢维年、刘克飞、刘爱华、张文璇、刘云龙、毕纪伟、田洪峰、初航、牛奔、邵林、唐晖、杨威、陈川、陈杰、王悦晞、郑立峰、姚彬、刘俊杰、曾德华、万玮、邢立立、刘广斌、肖伟。

区块链 专用服务网络 基础设施总体要求

1 范围

本文件规定了区块链专用服务网络基础设施的总体要求,包括基础层、支撑层、接入层、应用层、与外部节点的数据交换、运行维护、安全体系、监管机制等方面。

本文件适用于指导政府、事业和企业单位等开展专用网络环境中区块链系统的建设和服务运营。

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—2019 信息安全技术 网络安全等级保护基本要求

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4 分组密码算法

GB/T 32918.2—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法

GB/T 32918.3—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分:密钥交换协议

GM/T 0045—2016 金融数据密码机技术规范

GM/T 0054—2018 信息系统密码应用基本要求

GM/T 0059—2018 服务器密码机检测规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

区块 block

一种包含区块头和区块数据的数据结构。

注: 区块头包含前一个区块的摘要信息。

3.2

共识 consensus

在分布式节点间达成区块数据一致性的认可。

3.3

共识机制 consensus mechanism

在分布式节点间达成共识(3.2)的规则和程序。

3.4

共识算法 consensus algorithm

在分布式节点间为达成共识(3.2)而采用的计算方法。