ICS 35.240.01
CCS L70

团　体　标　准

T/CESA XXXX—202X

区块链基础设施 通用技术要求

Blockchain infrastructure - General technical requirement

征求意见稿

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

已授权的专利证明材料为专利证书复印件或扉页，已公开但尚未授权的专利申请证明材料为专利公开通知书复印件或扉页，未公开的专利申请的证明材料为专利申请号和申请日期。

202X-XX-XX 发布　　202X-XX-XX 实施

中国电子工业标准化技术协会　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。

本文件由北京微芯区块链与边缘计算研究院提出。

本文件由中国电子工业标准化技术协会区块链工作委员会归口。

本文件起草单位：。

本文件主要起草人：　。

区块链基础设施 通用技术要求

1 范围

本文件给出了区块链基础设施的总体框架，规定了区块链基础设施基础层、平台层、接入层、服务层以及安全管理和监管服务的技术要求。

本文件适用于区块链基础设施的设计、实施、使用和评估，为区块链基础设施开发、咨询服务、实施和测评等机构开展相关活动提供参考依据。

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。

GM/T 0054 信息系统密码应用基本要求

JR/T0184 金融分布式账本技术安全规范

T/CESA 1048 区块链 存证应用指南

T/CESA 1050 区块链 智能合约实施规范

T/CESA 1166 区块链 可装配系统 流程规范

T/CESA 1168 区块链 可装配系统 装配规范

T/CESA 1167 区块链 可装配系统 模块接口要求

T/CESA 6001 区块链 参考架构

3 术语和定义

JR/T0184、T/CESA 6001界定的以及下列术语和定义适用于本文件。

3.1

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人(例如接收者）伪造或抵赖。

[来源：GB/T 25069-2010，2.2.2.176]

3.2

区块链基础设施 blockchain infrastructure

一种基于区块链技术搭建的信息基础设施，涵盖网络、计算、存储等硬件设施，以及区块链技术基础平台、区块链服务接入能力，以及安全管理和监管服务，支持为各领域区块链应用场景提供技术服务能力。

4 缩略语

API 应用编程接口（Application Programming Interface）

AES	高级加密标准（Advanced Encryption Standard）
ECC	椭圆曲线加密算法（Elliptic Curve Cryptography）
ECDSA	椭圆曲线数字签名算法（Elliptic Curve Digital Signature Algorithm ）
SDK	软件开发工具包（Software Development Kit）

5 总体架构

区块链基础设施总体架构见图 1，包含基础层、平台层、接入层、服务层、安全管理、监管服务等六个部分。

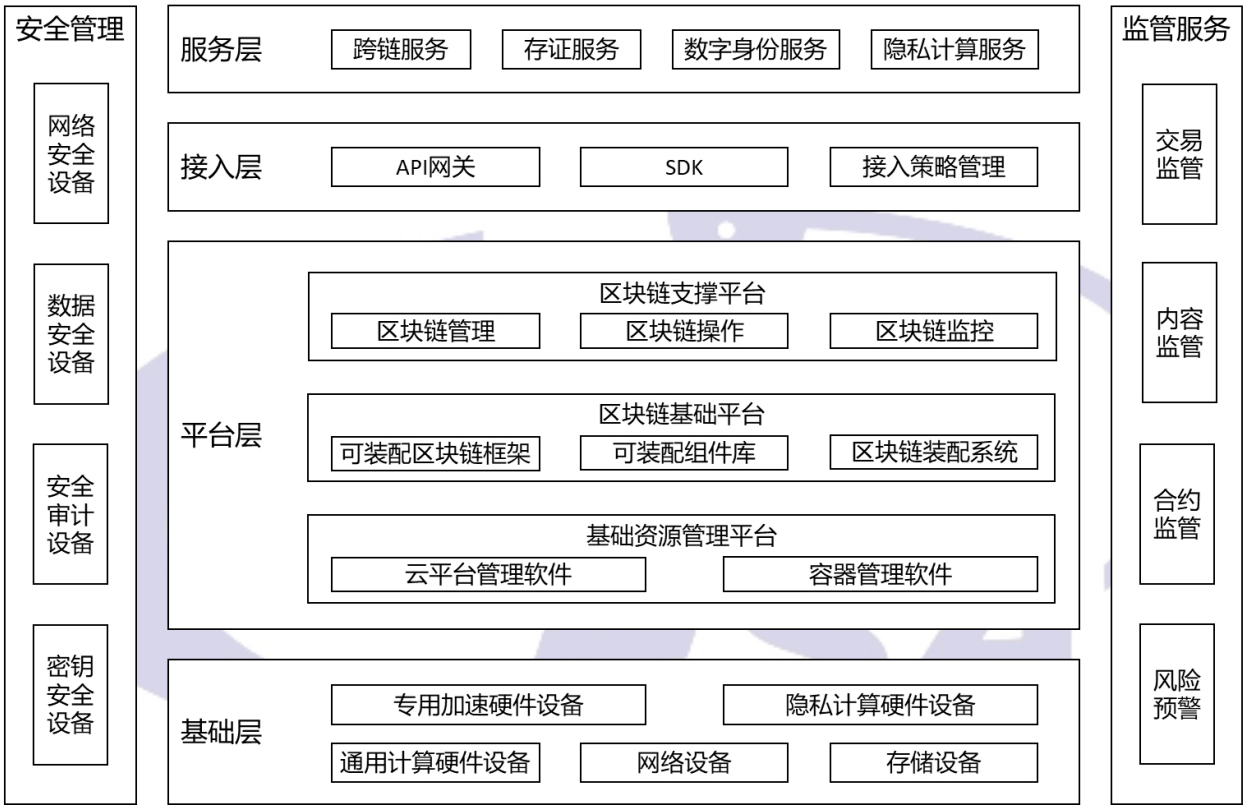

图 1 区块链基础设施总体技术架构

a）基础层：基础层提供必要的硬件运行环境，包括但不限于计算设备、网络设备、存储设备、隐私计算设备、加速设备等。

b）平台层：平台层提供构建、管理、操作、监控区块链平台的能力，以及开箱即用的区块链服务。平台层包括区块链基础平台、区块链支撑平台和基础资源管理平台。其中，区块链基础平台提供区块链基础能力，区块链支撑平台提供对区块链的管理、操作、监控等能力，基础资源管理平台负责进行云平台和容器的管理。

c）接入层：接入层提供区块链平台与应用之间的快速接入能力。接入层应对上层应用和服务提供API网关、多语言SDK等多种接入方式，提供接入策略管理和接入流量管理服务，管控上层应用和服务的接入访问权限和数据流量。

d）服务层：服务层提供基于区块链的共性基础服务，方便业务应用快速构建和对接。服务层包括跨链服务、存证服务、数字身份服务、隐私计算服务等，为业务应用提供同构链或异构链的跨链能力、基于区块链的存证取证能力、分布式数字身份的申请和使用能力、隐私计算能力等。

e）安全管理：安全管理指保障区块链基础设施系统安全的设备、技术、制度等，包括密钥安全、网络安全、存储安全、接入安全等。

f）监管服务：监管服务指针对区块链基础设施监管方提供的全方位的监管手段和机制，涵盖交易监管、内容监管、合约监管、风险预警等方面。

6 基础层

6.1 通用计算硬件设备

通用计算硬件设备为区块链基础设施的运行和服务提供通用计算能力，应满足以下要求：

a） 支持对区块链基础设施提供运行环境；

b） 支持满足区块链基础设施运行和性能要求；

c） 支持硬件设备虚拟化。

6.2 网络设备

网络设备为区块链基础设施提供网络连接和网络隔离能力，包括交换机、路由器、防火墙等。网络设备应满足以下要求：

a） 连接带宽达到区块链基础设施运行的最低标准；

b） 对区块链节点的点对点网络连接功能。

6.3 存储设备

存储设备为区块链基础设施提供数据存储能力，存储介质方面可分为机械硬盘、固态硬盘等，存储架构方面可分为磁盘阵列、分布式存储、软件定义存储等。存储设备应满足以下要求：

a） 存储容量能够满足区块链基础设施运行；

b） 存取速度能够满足区块链基础设施运行；

c） 能够高效、安全、稳定地提供数据写入及查询服务；

d） 支持按需动态添加和移除存储介质；

e） 支持数据高可用需要。

6.4 专用加速硬件设备

专用加速硬件设备为区块链基础设施提供密码运算加速、智能合约加速、共识算法加速等某一方面或某几方面的加速能力，包括加速芯片、加速板卡、加速一体机等。专用加速硬件设备应满足以下要求：

a) 在同等功耗下，对比通用硬件，可实现对区块链中某一方面或某几方面的加速；

b) 提供配套的驱动和开发工具；

c) 提供支持国密密码运算功能。

6.5 隐私计算硬件设备

专用加速硬件设备提供基于硬件的隐私计算能力，包括隐私计算板卡、一体机等。隐私计算设备应满足以下要求：

a) 具备基于硬件的隐私计算能力，可保护输入数据、输出数据、计算模型的隐私；

b) 提供配套的驱动和开发工具。

7 平台层

7.1 区块链基础平台

7.1.1 密码算法

密码算法是保障区块链基础平台底层安全的核心，一般包括对称加密算法、非对称加密算法、数字签名算法、摘要算法等。密码算法应满足以下要求：

a) 支持国际主流加密算法，如 AES 等对称加密算法，RSA、ECC 等非对称加密算法；

b) 支持我国商密加密算法，如 SM4 等对称加密算法，SM2 等非对称加密算法；

c) 支持国际主流数字签名算法，如 ECDSA；

d) 支持我国商密数字签名算法，如 SM2；

e) 支持国密主流摘要算法，如 SHA256；

f) 支持我国商密摘要算法，如 SM3；

g) 支持使用硬件密码设备进行密码算法计算。

7.1.2 共识机制

共识机制保障区块链基础平台节点之间的数据和状态严格一致，共识机制宜满足以下要求：

a) 具备一定的容错能力，在故障节点和恶意节点的比例不超过共识机制声明的容错率时，系统可正常运行；

b） 支持多个节点参与共识和确认，支持节点动态加入和退出共识算法；

c） 具备数据一致性，单一节点无法独立修改区块链网络中其他节点的数据；

d） 支持多种共识算法，可根据业务场景需求进行选择。

7.1.3 智能合约

区块链基础设施中对于智能合约的通用技术要求，参照 T/CESA 6001-2016中相关智能合约的有关规定。

7.1.4 账本管理

账本管理泛指区块链中分布式数据的存储机制，通过不同节点对账本的共同记录与维护，形成区块链系统中数据的公共管理、防篡改、可信任的机制。账本管理功能组件宜满足以下要求：

a） 支持持久化存储账本记录；

b） 按支持完整性校验的数据结构进行账本存储；

c） 支持多节点拥有完整的数据记录；

d） 支持向获得授权者提供真实的数据记录；

e） 确保有相同账本记录的各节点的数据一致性。

7.1.5 装配系统

为满足不同场景对区块链底层的差异化需求，区块链基础平台宜具备可装配能力，可根据需求装配不同特定的区块链底层。

装配系统的通用技术要求，参照T/CESA 1166、T/CESA 1167、T/CESA 1168中的相关规定。

7.2 区块链支撑平台

7.2.1 区块链管理

区块链管理负责区块链的新建和管理操作，宜满足以下要求：

a） 支持新建区块链操作，选择特定参与方创建一条区块链；

b） 支持链成员的添加和删除操作；

c） 支持链节点的添加和删除操作；

d） 支持链节点的启动和停止操作。