ICS
CCS 点击此处添加 CCS 号

团　　体　　标　　准

T/GZBIA XXXX—XXXX

政务区块链技术安全规范

Security Specification for Government Blockchain Technology

（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。

××××－××－××发布　　××××－××－××实施

广州市区块链产业协会　　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。

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。

本文件由广州市区块链产业协会提出。

本文件由广州市区块链产业协会归口。

本文件起草单位：

本文件主要起草人：

政务区块链技术安全规范

1 范围

本标准规定了政务区块链技术的安全通用要求，涵盖区块链基础设施、核心功能、服务接口、应用、治理、跨层、硬件设施等核心环节的安全要求。

本标准适用于指导政务区块链系统的规划、设计、开发、部署、运维及安全监管等。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 25070-2019 信息安全技术 网络安全保护安全设计技术规范

GB/T 22239-2019 信息安全技术 网络安全保护基本规范

GB/T 43572-2023 区块链和分布式记账技术 术语

GB/T 42752-2023 区块链和分布式记账技术 参考架构

GB/T 42570-2023 信息安全技术 区块链技术安全框架

GB/T 42571-2023 信息安全技术 区块链信息服务安全规范

GB/T 25069信息安全技术指南、可信计算标准，GB/T 31168云计算安全指南

3 术语和定义

下列术语和定义适用于本文件。

3.1 区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

[来源：GB/T 43572-2023/ISO 22739:2020，定义3.6]

3.2 非对称加密算法 asymmetric encryption algorithms

用于公钥和私钥对数据的存储和传输的加密和解密的一种算法。其在区块链的应用场景主要包括信息加解密、数字签名与验签等。区块链系统中，涉及到非对称加密算法主要有RSA算法、D-H算法、ECC算法等。

3.3 交易 transactions

工作流程的最小单位，是产生符合控制规则的结果所需的一个或多个活动序列。

[来源：GB/T 43572-2023/ISO 22739:2020，定义3.77]

4 政务区块链技术安全架构

政务区块链技术安全架构涵盖基础设施安全层、核心功能安全层、服务接口安全层、应用安全层、治理安全层和跨层安全，见图1。

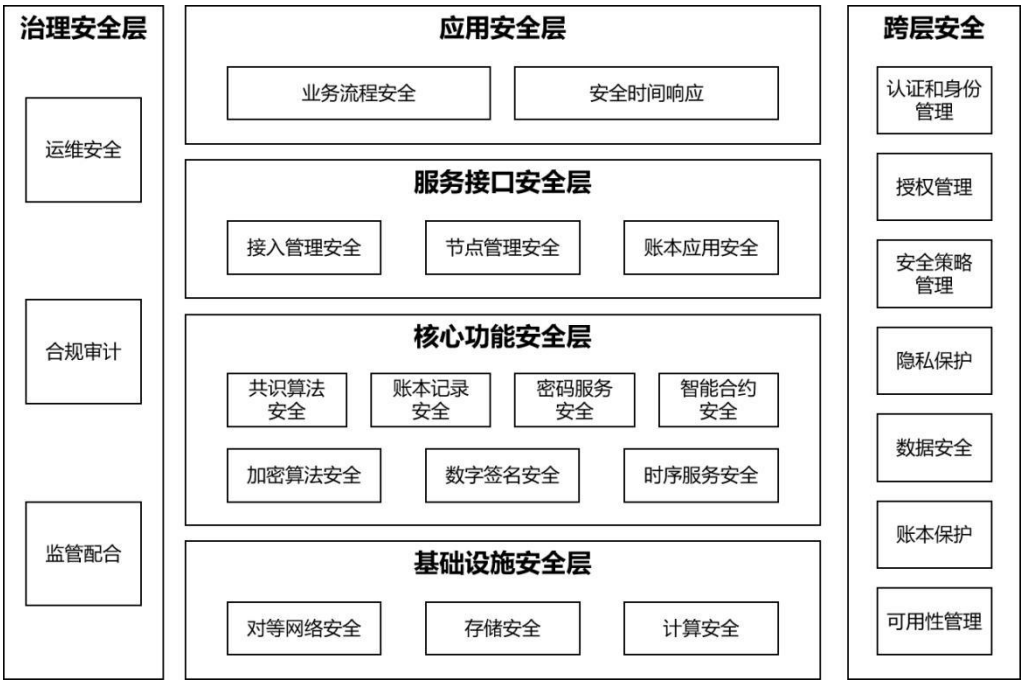

图1 政务区块链技术安全架构

5 基础设施安全层

5.1 对等网络安全

政务区块链系统运行的底层拓扑结构是分布式对等网络，采用对等网络协议组织政务区块链中的各个网络节点，各个节点间通常使用点对点通信协议完成信息交换以支撑上层功能。对等网络安全应符合：

a） 节点身份认证，通过安全的身份认证机制确认其合法性，防止未授权节点加入网络；

b） 通信数据加密，节点之间的数据通信应使用强加密算法进行保护，确保数据的保密性和完整性，防止信息被窃听或篡改；

c） 安全路由机制，具备防护能力的路由协议，有效抵御路由欺骗、流量重定向和拒绝服务攻击；

d） 访问控制，配置严格的访问控制策略，确保不同节点的访问权限符合政务系统的需求，并避免权限滥用；

e） 网络拓扑动态调整，适应节点的增减和网络变化，同时保证系统的稳定性与安全性；

f） 抗分区攻击，确保即使在分区情况下，数据一致性和网络功能依然得以维护；

g） 定期协议更新，支持版本升级和安全补丁的发布，及时修复已知漏洞，提升整体安全性。

5.2 存储安全

存储功能组件提供政务区块链运行过程中产生的各种类型数据的写入及查询功能。存储安全符合：

a） 应具备数据完整性保障，支持建立数据完整性校验机制（如Merkle Tree）来防止数据篡改；

b） 应具备数据一致性保障，支持数据写入前校验和写后校验功能，确保写入过程中的数据一致性；

c） 应具备数据加密存储，支持在区块链底层的数据应进行静态加密；宜采用符合国家密码标准（如SM4）的加密算法；

d） 应具备不同类型数据的数据分级加密策略，确保政务敏感数据具有更高的安全保护级别；

e） 应支持细粒度的访问控制机制，确保只有授权节点或角色能够执行数据读取和写入操作；

f） 应具备存储冗余和容灾备份，具备跨地域的数据备份和灾难恢复能力，确保在发生硬件或网络故障时数据依然可用。

5.3 计算安全

计算功能组件提供政务区块链系统运行中的计算能力支持，包括但不限于容器技术、虚拟机技术、云计算技术等。计算安全符合：

a） 若使用容器或虚拟机技术，应提供强隔离的计算环境，防止不同容器或虚拟机之间的资源越界访问；应采用轻量级虚拟化技术（如容器沙箱）来增强隔离性，同时降低计算开销；

b） 宜支持计算过程中的数据加密（如内存加密、计算时加密），防止敏感数据在计算过程中被窃取或篡改；

c） 对于跨节点的计算任务，应支持基于多方安全计算（MPC）的安全协议，确保分布式计算结果的安全性和正确性；

d） 应具备计算任务调度的访问控制机制，支持对计算任务的调度过程进行日志记录和审计；

e） 应具备抗拒绝服务（DoS/DDoS）能力，防止外部恶意节点通过计算请求耗尽系统资源；应具备流量限制策略和资源配额机制，确保每个节点的计算资源分配合理，防止资源滥用；

f） 宜兼容主流国产化软硬件；

g） 宜采用可信执行环境（Trusted Execution Environment，TEE）技术，确保敏感计算任务在可信硬件中执行，防止外部攻击。

6 核心功能安全层

6.1 共识算法安全

共识算法是提供政务区块链系统中各节点达成一致性协议的机制。共识算法安全符合：

a） 应具备抗分叉能力和双花攻击防护，确保共识结果的唯一性和正确性；

b） 应具备共识协议容错能力，保障一定比例节点失效或恶意行为情况下，保持系统运行的可靠性与一致性；

c） 应支持共识过程中消息传递的加密和签名机制，防止共识消息被窃听或篡改；

d） 应具备共识节点的身份认证机制，确保只有合法节点参与共识过程；

e） 应支持关键操作的日志记录和审计，确保出现异常情况时能够溯源；

f） 宜支持共识算法动态升级，确保在新的安全威胁出现时及时调整共识策略。

6.2 账本记录安全

账本记录提供政务区块链系统中交易数据的存储与查询功能。账本记录安全符合：

a） 应提供账本数据的不可篡改性保障，确保数据完整性；

b） 应具备账本数据的分层访问控制机制，支持不同角色仅能访问其授权范围内的数据；

c） 应支持账本数据存储加密，支持符合国家标准的加密算法（如SM4）进行静态加密；

d） 账本数据变更时，应支持链上多签或多方授权机制，确保数据变更过程的安全性；

e） 应具备账本快照和备份机制，确保在出现系统故障或攻击时能够快速恢复账本状态；

f） 宜支持账本的审计功能，定期输出账本安全状态报告。

6.3 密码服务安全

密码服务提供政务区块链系统中的加密、解密、签名、验签等基础密码运算能力。密码服务安全符合：

a） 应采用符合国家密码标准的算法（如SM2、SM3、SM4），确保密码算法的安全性和合规性；

b） 应提供密码密钥的安全存储与管理机制，支持密钥的生成、分发、使用、销毁等生命周期管理；

c） 应具备抗侧信道攻击能力的密码运算，防止通过电磁、功耗等物理攻击窃取密码信息；

d） 应具备密钥操作的权限控制和操作日志记录，确保密钥操作过程可追溯；

e） 宜支持硬件密码模块（HSM），确保高强度密码操作的性能与安全；

f） 宜支持密码算法的在线升级，确保密码算法在面对新威胁时能够及时更新。

6.4 智能合约安全

智能合约提供政务区块链系统中链上逻辑执行的能力。智能合约安全符合：

a） 应提供智能合约的安全检测机制，支持合约部署前的静态分析和运行时的动态监测，防止常见漏洞（如重入攻击）；

b） 应支持智能合约的权限管理机制，确保合约调用仅由授权用户发起；

c） 应具备合约执行的资源限制机制，防止因恶意合约导致的资源耗尽攻击；

d） 应具备智能合约操作的日志记录和审计功能，确保异常行为可追溯；

e） 应支持智能合约的版本管理和升级机制，确保在发现合约漏洞时可快速修复；

f） 宜采用形式化验证技术，对关键智能合约进行形式化验证，确保合约行为的正确性。

6.5 加密算法安全

加密算法提供政务区块链系统中数据加密、解密的基础能力。加密算法安全符合：

a） 应采用符合国家标准的加密算法（如SM2、SM3、SM4）进行数据加密，确保算法的安全性与合规性；

b） 应提供加密算法的版本管理机制，支持在新算法发布或现有算法被破解时快速替换；

c） 宜具备加密过程的抗量子攻击能力，宜采用抗量子密码算法或密钥扩展机制；

d） 应具备加密操作的权限控制和操作日志记录功能，确保加密过程可审计；

e） 宜支持硬件加速模块，提高加密运算的效率与安全性。

6.6 数字签名安全

数字签名提供政务区块链系统中身份认证与数据完整性校验的能力。数字签名安全符合：

a） 应采用符合国家标准的签名算法（如SM2）进行签名与验签，确保签名算法的安全性；

b） 应具备签名密钥的强随机性和高强度，采用硬件安全模块（HSM）进行生成和存储；

c） 应支持基于证书的签名机制，确保签名身份的真实性与可验证性；

d） 应具备签名操作的权限控制和操作日志记录功能，确保签名过程可审计；

e） 宜支持数字签名算法的在线升级，确保在发现漏洞时及时更新；

6.7 时序服务安全

时序服务提供政务区块链系统中时间戳管理与验证的能力。时序服务安全符合：

a） 应提供精确的时间同步机制，支持与可信时间源（如北斗授时系统）的同步，确保时间戳的准确性；

b） 应具备时间戳服务的防篡改能力，确保生成的时间戳不可伪造；

c） 应具备时间戳操作的权限控制与日志记录功能，确保时间戳生成与使用过程可追溯；

d） 宜支持分布式时序服务架构，确保在单点故障情况下时序服务的高可用性；

e） 宜支持基于区块链的时间戳链，确保时间序列的完整性和可验证性。

7 服务接口安全层

7.1 接入管理安全

接入管理提供政务区块链服务接口层对外部系统或节点接入的控制与管理。接入管理安全符合：

a） 应具备强身份认证机制，采用双因素认证、多因素认证等手段确保接入方身份的真实性；

b） 应采用加密通信（如TLS）机制，防止传输数据被窃取或篡改；

c） 应支持基于角色的访问控制（RBAC），支持基于属性的访问控制（ABAC），确保不同接入方的权限隔离；

d） 应具备接入过程的动态风控能力，对异常接入行为实时监控与阻断；

e） 应支持对所有接入操作进行日志记录与审计，确保接入行为可追溯；

f） 宜支持接入流量的限速与熔断策略，防止因外部异常请求导致系统资源耗尽。

7.2 节点管理安全

节点管理提供政务区块链网络中各节点的运行与维护。节点管理安全符合：

a） 应具备节点身份认证机制，确保只有合法节点能够加入政务区块链网络；

b） 节点间的通信应采用端到端加密，防止通信内容被窃取或篡改；

c） 应具备节点运行状态监控与异常检测机制，确保节点异常时及时报警并处理；

d） 节点管理操作应具备权限控制与审计功能，确保节点操作安全可追溯；

e） 宜支持基于共识的节点准入机制，防止恶意节点随意加入系统；

7.3 账本应用安全

账本应用提供政务区块链上各类账本应用的运行与使用。账本应用安全符合：

a） 应具备账本数据的访问控制机制，确保不同用户或应用仅能访问其授权范围内的数据；

b） 宜支持账本操作的多方签名机制，确保重要数据操作的安全性与可靠性；

c） 应具备账本应用的操作日志记录与审计功能，确保应用操作行为可追溯；

d） 宜采用链上链下联合存储机制，确保敏感数据在链上处理而非敏感数据在链下存储时仍具备高安全性；

e） 宜支持账本应用的动态升级，确保在发现漏洞时可快速修复。

8 应用安全层

8.1 业务流程安全

业务流程安全涉及应用层中各类业务流程的执行与控制，确保政务区块链的业务操作安全性与合规性。业务流程安全符合：

a） 应对关键业务流程操作设置多方审批机制，确保重要操作的可靠性与合规性；

b） 应具备业务流程的完整性校验与异常检测机制，防止业务流程被篡改或恶意中断；

c） 应具备业务流程操作的实时监控与报警能力，对异常行为及时预警与处理；

d） 应支持业务流程的自动化存证与审计，确保业务流程的可追溯性与可信性；

e） 宜支持基于智能合约的业务流程自动执行与校验，减少人工干预带来的安全风险。

8.2 安全事件响应

安全事件响应提供政务区块链的应用安全事件监控、处理与恢复，确保系统在发生安全事件时能够快速响应与恢复。安全事件响应符合：

a） 应具备实时安全事件监控与报警机制，确保在发生异常时能够及时预警；

b） 应具备自动化应急响应机制，对常见安全事件进行快速处理与隔离；

c） 应支持安全事件的日志记录与溯源分析，确保事件处理过程可追溯；

d） 宜具备安全事件的恢复与修复能力，确保系统在发生安全事件后能够快速恢复正常运行；

e） 宜支持安全事件响应预案的定期演练与优化，确保预案的有效性。

9 治理安全层

9.1 运维安全

运维安全涉及政务区块链系统的运行与维护管理，确保系统稳定、安全地运行。运维安全符合：

a） 应具备严格的运维访问控制机制,对运维人员的操作权限进行精细化管理,确保最小权限原则；

b） 应对所有运维操作进行实时监控与日志记录，并支持日志的集中存储与审计，确保运维行为可追溯；

c） 应采用多因素认证机制，确保运维人员身份的真实性与安全性；

d） 应具备运维工具的安全性检测与认证，确保运维工具无恶意代码或漏洞；

e） 应具备运维任务的自动化与审计能力，减少人工干预带来的安全风险；

f） 宜支持基于区块链的运维流程存证与验证，确保关键运维操作过程透明、可信。

9.2 合规审计

合规审计提供对政务区块链系统的运行合规性进行检查与评估,确保系统符合相关法律法规及标准。合规审计符合：

a） 应具备合规审计机制，定期对系统的运行状态、数据存储、访问行为等进行审计与评估；

b） 应采用审计记录的链上存证技术，确保审计结果的完整性与不可篡改性；

c） 应支持多维度合规审计，包括但不限于数据合规、操作合规、隐私保护合规等方面；

d） 宜支持审计报告的自动生成与多方校验机制，确保审计结果的权威性与透明性；

e） 宜支持外部第三方审计，确保系统合规性评价的独立性与客观性。

9.3 监管配合

监管配合提供政务区块链系统与监管机构之间的数据共享与管理支持，确保系统符合监管要求。监管配合符合：

a） 应具备合规的数据共享机制，对接监管机构提供必要的数据接口，确保数据真实、完整；

b） 应支持数据共享的访问控制与权限管理，确保不同监管机构仅能访问授权范围内的数据；

c） 应支持基于区块链的多方监管机制，确保监管过程透明化与可信化；

d） 对于敏感数据的监管访问，应具备安全隔离与隐私保护机制，确保在满足监管要求的前提下保障用户隐私；

e） 宜支持智能合约驱动的自动化监管机制，在监管规则触发时自动进行记录与预警；

f） 宜采用区块链联盟链架构，确保监管机构能够实时、透明地获取系统运行状态与关键信息。

10 跨层安全

10.1 认证和身份管理

认证和身份管理提供政务区块链系统中所有用户与节点的身份认证与管理，确保身份的真实性与唯一性。认证和身份管理安全符合：

a） 应支持统一的身份认证机制，确保所有层次的用户与节点身份认证一致性；

b） 应采用基于密码学的身份认证机制（如数字证书、数字签名）进行强认证，确保身份的防伪性与安全性；

c） 应支持跨链身份互认证，确保不同链之间的身份可验证性与互通性；

d） 宜支持基于去中心化身份（DID）的身份管理模式，确保身份管理的分布式与自主性；

e） 宜具备身份生命周期管理机制，支持身份的注册、更新、撤销与注销。

10.2 授权管理

授权管理提供对政务区块链系统中不同用户、节点与应用的权限分配与控制，确保权限分配合理与安全。授权管理符合：

a） 应具备精细化的权限管理机制，支持对不同角色的操作权限进行分级授权；

b） 应支持动态权限管理机制，确保权限在系统状态变化时能够自动调整；

c） 应对敏感操作设置多因素授权机制，确保高风险操作的安全性；

d） 应具备授权过程的日志记录与审计能力，确保授权行为可追溯；

e） 宜采用基于属性的访问控制（ABAC）机制，支持基于多维属性的灵活授权策略。

10.3 安全策略管理

安全策略管理提供政务区块链系统中安全策略的制定、执行与更新，确保安全策略的一致性与有效性。安全策略管理符合：

a） 应具备统一的安全策略配置中心，支持各层安全策略的集中管理与分发；

b） 应支持安全策略的动态调整与自动化执行，确保策略在环境变化时的适应性；

c） 应对安全策略的配置与调整进行完整的日志记录，确保策略变更过程可追溯；

d） 宜具备基于策略的安全事件响应机制，确保在策略触发条件下自动预警与处理；

e） 宜采用策略模型化管理，支持策略的形式化验证与优化。

10.4 隐私保护

隐私保护提供政务区块链系统中用户数据的隐私管理与控制。隐私保护符合：

a） 应具备隐私数据的分级分类管理机制，对不同级别的隐私数据采用不同的保护策略；

b） 隐私数据存储应采用符合国家标准的加密算法，并支持敏感数据的脱敏处理；

c） 应具备隐私数据的访问审计机制，对所有隐私数据的访问与操作行为进行日志记录与审计；

d） 应支持链上隐私保护协议（如零知识证明、环签名等），确保隐私数据在链上交互时的安全性；

e） 宜采用隐私增强计算技术（如同态加密、差分隐私）进行数据处理，确保隐私数据的安全计算；

10.5 数据安全

数据安全提供政务区块链系统中用户数据的安全存储、传输与使用。数据安全符合：

a） 应对所有存储数据进行加密处理，采用符合国家标准的加密算法（如SM4）；

b） 数据传输应采用加密通道，确保传输过程中的数据安全性；

c） 应具备数据完整性校验机制，确保存储与传输过程中的数据未被篡改；

d） 应支持数据备份与恢复机制，确保系统在发生故障或攻击时能够快速恢复；

e） 宜支持数据的动态加密与解密，确保在数据使用过程中始终保持安全性；
f） 宜支持数据生命周期管理机制，对数据的生成、使用、存储、销毁等环节进行全程管控。

10.6 账本保护

账本保护提供对政务区块链系统核心账本的完整性与一致性保护，确保账本数据的安全与可信。账本保护符合：

a） 应采用链上数据加密机制，确保账本中敏感数据的保密性；
b） 应具备账本数据的完整性校验机制，防止账本数据被恶意篡改；
c） 应对账本的访问设置严格的权限控制，确保只有授权用户与节点可以读取与操作账本；
d） 应支持账本快照与备份机制，确保在发生安全事件时能够快速恢复账本状态；
e） 宜支持账本历史版本管理与查询，确保账本变更过程可溯源与可验证。

10.7 可用性管理

可用性管理提供政务区块链系统在高负载或异常情况下的稳定运行与服务可持续性,确保系统持续可用。可用性管理符合：

a） 应具备负载均衡机制，确保在高并发访问情况下系统能够平稳运行；
b） 应具备异常检测与自动恢复能力，确保系统在发生异常时能够快速恢复正常运行；
c） 应对关键节点与服务设置高可用冗余机制，防止单点故障导致系统不可用；
d） 应具备抗拒绝服务（DoS/DDoS）攻击能力，确保系统在遭受外部攻击时能够持续提供服务；
e） 宜采用基于区块链的共识容错机制，确保在部分节点失效情况下系统能够正常运行。

11 硬件设施安全要求

11.1 计算设备

节点的计算硬件提供政务区块链的计算能力，以支持政务区块链系统中复杂的共识算法、密码计算及智能合约执行等。具体要求如下：

a） CPU宜支持硬件级加密加速指令集（如AES-NI、SHA指令集），提高加密和解密运算效率；
b） 对于高性能节点，建议使用多核高频处理器，以提高并行处理能力；
c） 宜支持异构计算加速（如GPU或FPGA），以加速密码学运算与智能合约的执行。

11.2 存储设备

节点的存储硬件提供政务区块链的存储能力，支持大规模数据长期保存，具备高容量、高可靠性与高性能的特点。具体要求如下：

a） 应使用企业级存储设备，提供冗余与容错机制，确保数据的高可靠性；
b） 应具备加密存储功能，确保账本与关键数据的保密性；
c） 宜支持分布式存储架构，确保账本数据存储的扩展性与可用性；
d） 存储介质宜采用固态硬盘（SSD）以提高数据读写速度。

11.3 网络设备

节点的网络设备提供政务区块链系统节点的互联互通，具备高带宽、低延迟与强抗攻击能力。具体要求如下：

a） 应支持千兆或万兆以太网接口，确保节点间通信的高带宽；

b） 应具备DDoS攻击防护能力，支持流量清洗与攻击防护策略；
c） 应支持VPN或专线通信，确保节点间通信的机密性与完整性；
d） 宜采用多链路冗余设计，确保网络的高可用性与容灾能力。

11.4 硬件安全模块（HSM）

为确保密钥的安全管理，政务区块链系统配备硬件安全模块（HSM），要求如下：
a） 应符合国际安全标准（如FIPS 140-2或以上级别）认证，确保其安全性；
b） 应支持主流密码算法（如国密SM2、SM3、SM4以及RSA、ECDSA等）；
c） 应具备密钥生成、存储、使用及销毁的全生命周期管理能力；
d） 应支持与区块链节点的集成接口，确保密钥操作在HSM中完成，防止密钥泄露。

11.5 可信执行关键（TEE）

为提高敏感数据处理的安全性，政务区块链系统的关键节点配备可信执行环境（TEE），要求如下：
a） 硬件应支持可信执行环境（如Intel SGX、ARM TrustZone），确保敏感计算任务的隔离执行；
b） 应具备内存加密与访问控制功能，防止敏感数据在运行过程中被窃取；
c） 宜支持远程证明机制，确保其他节点能够验证TEE的可信状态。

11.6 电源与环境要求

政务区块链系统需长期稳定运行，硬件设施应具备电力冗余与环境适应能力。具体要求如下：
a） 应配备不间断电源（UPS）与备用电源，确保在电力中断时系统持续运行；
b） 机房应具备温湿度监控与自动调节系统，确保硬件设备在最佳环境下运行；
c） 宜具备消防与防水设施，确保硬件设施的物理安全性。