ICS 35.020
CCS L 70

团 体 标 准

T /CIITA 401-2021

区块链 关键服务 安全技术要求

Blockchain—critical service—technical specifications for security

2021-12-22 发布 2022-01-22 实施

中国信息产业商会 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。

本文件由中国信息产业商会提出并归口。

本文件起草单位：西安四叶草信息技术有限公司、深圳零时科技有限公司、西北大学、西安灵动计算机系统有限公司、北京知道创宇信息技术股份有限公司、中国信息产业商会信息安全分会、成都信息工程大学。

本文件主要起草人：孙骞、童小敏、邓永凯、赵培源、朱利军、刘艺琨、张继龙、晏梓桐、李辉、张臻、李军、翟瑞飞、马坤、郑玮、彭丽、张进、姚昌林、肖龙、朱程、李鹏轩、田铭、武成军、田昊、郑庆霄、刘庆麟、闫博、李冬芸、孙雪萌。

本文件为 2021 年第一次发布。

引　言

习近平总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新重要突破口，加快推动区块链技术和产业创新发展。党的十九大报告指出，要“加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间”。中共中央政治局 2021 年 11 月 18 日召开会议，审议《国家安全战略（2021－2025 年）》，会议强调必须坚持把政治安全放在首要位置，统筹做好政治安全、经济安全、社会安全、科技安全、新型领域安全等重点领域、重点地区、重点方向国家安全工作；会议还提出，要加快提升生物安全、网络安全、数据安全、人工智能安全等领域的治理能力。

国务院办公厅《关于以新业态新模式引领新型消费加快发展的意见》（国办发〔2020〕32 号）、国家发展改革委会等 28 部门联合颁布的《加快培育新型消费实施方案》（发改就业〔2021〕396 号）的联动部署中，要求“加强信息网络基础设施建设，大力推动智能化技术集成创新应用，在有效防控风险的前提下，推进大数据、云计算、人工智能、区块链等技术发展融合”。区块链技术和产业在快速发展的同时，区块链应用服务的安全需求也更加迫切。

本文件针对普遍使用区块链技术的网络信息系统设计、建设、运行等急需的安全保障，特别是公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技、工业互联网等重要行业和领域，规定了使用区块链技术进行关键服务的内容、安全技术要求，适用于使用区块链技术进行相关应用的系统设计、系统建设、系统运行。

区块链 关键服务 安全技术要求

1 范围

本文件规定了使用区块链技术进行关键服务的内容和安全技术要求。

本文件适用于使用区块链技术进行相关应用的系统设计、系统建设、系统运行。

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，仅所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 25069-2010 信息安全技术 术语

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式

3 术语和定义

GB/T 25069-2010、GB/T 20270-2006 和 GB/T 39786-2021 中界定的以及下列术语和定义适用于本文件。

3.1

关键服务 critical service

基于智能合约、数字钱包、联盟链、分布式文件存储等区块链技术，融入国家安全、国计民生、公共利益等重要行业和领域信息系统设计、建设和运行的定制应用。

3.2

区块链 blockchain

一种在对等网络环境下，通过透明和可信规则，构建防伪造、防篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

3.3

安全技术 security technology

基于本文件第 2 章标准要求的，并不限于第 2 章的网络信息安全综合技术。

3.4

智能合约 smart contract

以数字形式定义的、能够自动执行条款的计算机程序。

3.5

钱包 wallet

区块链技术中用于存储用户私钥的软件或者硬件。

3.6

联盟链 consortium blockchain

由一组具有利益相关的特定授权用户使用，仅有授权节点可接入，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。

3.7

私有链 private blockchain

仅由单个区块链服务客户使用，仅有授权的该客户节点可接入，接入节点可按规则参与共识和读写数据的一类区块链部署模型。

3.8

分布式账本 distributed ledger

在多个站点、不同地理位置或者多个机构组成的网络里实现共同治理及分享的资产数据库。

3.9

节点 node

区块链服务中独立运行的一种基本单元。

3.10

对等网络 peer-to-peer network

一种包含同等地位的节点的计算机网络。

3.11

共识算法 consensus algorithm

区块链技术中各节点为达成一致采用的计算方法。

3.12

基础设施 infrastructure

支持区块链技术应用的网络设施、信息系统、数据存储、算法等。

3.13

虚拟机 virtual machine

某个特定用户独占使用的一种虚拟的数据处理系统。

4 缩略语

下列缩略语适用于本文件。

DAPP 去中心化应用（decentralized application）

DDOS 分布式拒绝服务（distributed denial of service）

DNS 域名解析服务器（domain name resolution）

EFS 加密文件系统（encrypted file system）

HTTPS 安全超文本传输协议（hyper text transfer protocol over secure socket layer）

IPS 入侵防御系统（intrusion prevention system）

P2P 点对点技术（point-to-point technology）

SSL 安全套接字协议（secure sockets layer）

WAF 网站应用级入侵防御系统（web application firewall）

5 关键服务

将存证防伪、可溯源和自动价值流转，作为本文件定制的、使用区块链技术的关键服务内容。

5.1 存证防伪

通过区块链技术的数字签名和链上存证可以对文字、图片、音频、视频等数字内容进行确权，并可证明存在于特定时间的，其公开、不可篡改、可溯源等特性，促进了区块链技术服务的广泛应用。

5.2 可溯源

通过区块链技术保证参与者无法篡改账本，确保交易记录透明安全，监管部门方便地追踪链上交易，快速定位高风险交易。

5.3 自动价值流转

在保护数据隐私的前提下实现多方协作的数据计算，解决“数据垄断”和“数据孤岛”问题，实现数据流通价值。

6 安全要求

应以相应的技术手段，以及这些手段导入网络信息系统安全技术、密码技术、数据存储技术、智能合约技术、钱包技术、联盟链技术、分布式存储技术的应用，保障所提供的关键服务，能够匹配及保障系统设计、系统建设、系统运行的安全状态。

6.1 网络信息系统安全技术

应将保障网络信息系统的安全，作为保障实现关键服务的必要条件。必要条件见附录A。

6.2 密码技术

应将保障网络信息系统的安全和保障实现关键服务安全的密码技术应用，作为必要条件。保障密码技术应用安全的必要条件见附录 B。

6.3 数据存储技术

6.3.1 安全要求

a） 制定用户个人信息和账本信息存储策略，明确信息存储方式、存储流程、同步方式等关键要素；
b） 系统日志的留存时间应不少于 6 个月；
c） 对存储的重要数据进行定期备份，避免同一物理空间的备份；
d） 对交易内容进行留存，包括区块数据、账户数据、共识数据等；
e） 保证数据存储空间的存储能力，防止数据量过大耗尽存储空间而导致数据的丢失；
f） 应有审计追踪机制，对数据的更新修改等要有日志记录，确保数据安全；
g） 备份的重要数据需要经过加密存储，防止备份数据被窃取造成用户数据泄漏。

6.3.2 专用硬件要求

针对区块链采用的 FPGA/ASIC 等专用硬件，包括密码算法、智能合约等加速硬件，安全要求如下：

a） 专用硬件与其他节点通信时，要建立安全的通信通道，要对关键数据信息进行加密传输；
b） 处理敏感信息的专用硬件具有缓解物理侧信道攻击的能力，防止保密信息被窃取；

c） 数据应存储在硬件环境安全性较高的数据库中，可使用基于内存加物理存储的架构以及key-value 的存储引擎。

6.3.3 可信执行环境

可信执行环境安全要求如下：

a） 同一平台的可信环境之间能相互验证彼此运行在同一平台之上，自证自身代码和数据的完整性，验证对方的平台环境和自身的完全一致；

b） 可信环境可以使得除自己之外的第三方能验证可信环境的代码和数据未被恶意篡改，且运行在预期的硬件平台上。只有验证通过后，第三方才向可信环境提供相关敏感数据。

6.4 智能合约技术

6.4.1 基础设施安全

6.4.1.1 虚拟机安全

虚拟机安全是智能合约安全的重要内容，合约执行功能的正确性、安全性都与之密切关联，具体安全要求：

a) 能够安全处理异常调用；
b) 不存在虚拟机逃逸漏洞；
c) 不存在任意代码执行漏洞；
d) 不存在 DOS 漏洞；
e) 预编译合约（内建合约、系统合约）调用与执行安全。

6.4.1.2 交易节点安全

智能合约通过交易的形式在节点上部署和执行，而节点则会开放接口供外部调用或查询合约，节点需做好必要的安全防护，确保主机安全。具体安全要求：

a) 区块链系统（节点）需要做好安全防护，保障主机安全；
b) 区块链系统（节点）需要防止已部署合约代码被任意篡改；
c) 提供合约查询和调用的节点需确保自身状态正确；
d) 防止合约部署或调用占用节点过多计算资源；
e) 防止合约部署或调用引起节点崩溃；
f) 能够正常防范针对节点发起的其他形式的攻击。

6.4.2 安全服务功能

6.4.2.1 形式化验证

智能合约的形式化验证应包含合约制定、形式描述、建模验证、代码生成和一致性测试等一系列过程测试验证智能合约代码的正确性。

a) 应按照需求约定形式规范来设计合约，编写智能合约文本；
b) 应根据智能合约模型描述和性能描述要求，对文本进行形式化描述；
c) 应选择合适的建模语言和工具对形式化描述进行建模和验证；
d) 将验证模型生成符合形式化描述的标准化合约代码；
e) 生成代码与标准合约文本进行一致性测试。

6.4.2.2 调用安全

a) 应具备对智能合约的操作权限设置功能，遵循权限最小化原则，对外公开接口应将其能进行的操作最小化；
b) 合约间相互调用时，应使用“检查-生效-交互”模式；
c) 对接口访问权限进行等级划分，针对不同用户配置不同的访问权限；
d) 接口接入应明确参数类型、数量及输入信息，接口返回数据应明确数据类型、数量及输出信息；
e) 接口描述文件应为预言机提供的结构化描述语言，接口协议应包含安全传输协议。

6.4.2.3 合约版本安全

a) 智能合约的每次修改应为独立版本，并在源代码中通过区块链平台指定方式定义版本号；
b) 若在配置文件中定义版本号，该配置文件需要与智能合约代码一同部署。

6.4.2.4 合约升级安全

a) 智能合约的升级操作应由客户端发起，以接口调用方式在区块链中提交，达成共识生效；
b) 合约升级后区块链中应保留前一版本，区块中记录的交易信息中应明确交易调用的合约版本。

6.4.2.5 合约编码安全

a) 智能合约代码应符合安全编码规范要求，包含代码书写规范、逻辑要求等，应使用广泛应用的安全技术和工具进行风险分析；
b) 合约和函数应模块化，逻辑简洁，不宜使用过时的语法，避免已知的逻辑漏洞和错误，如转账前余额未校验，未检查返回值的调用等；
c) 智能合约应使用已经广泛应用的合约语言，宜采用最新的稳定版本，确保编程语言与编译器的一致性，合约源码在编译成字节码之后应保证前后逻辑一致性。

6.4.2.6 安全审计

智能合约的安全审计和评估对象应包括智能合约设计与业务逻辑安全、源代码安全审计、编译环境审计及相关的应急响应措施等；

a) 应对智能合约的业务逻辑、业务流程进行安全性测试和评估；
b) 应利用审计工具和人工审阅相结合的方式对代码漏洞进行逐项分析检查；
c) 应通过人工观察智能合约编译器的名称和版本，识别有漏洞的版本；
d) 应具备应急响应措施，发现漏洞后及时检查和修复合约源代码。

6.4.3 安全运行管理

6.4.3.1 合约部署安全

a) 应具备相应机制控制智能合约的部署行为，防止恶意部署智能合约；
b) 应提供运行载体，保证智能合约运行环境与外隔离。

6.4.3.2 合约实例化安全

a) 应校验智能合约的实例化实体、通道写入策略和签名；
b) 将合约状态作为合约账户的属性、合约内容的哈希值保存在区块链网络；
c) 在运行智能合约前，应检查该智能合约和链上智能合约哈希值的一致性。

6.4.3.3 合约执行安全

a) 合约在智能合约运行时环境中的执行结果应具备事务一致性；
b) 当智能合约出现错误时，宜提供智能合约挂起或重启恢复功能。

6.4.3.4 合约废止安全

a) 调用智能合约废止时，应进行权限访问控制；
b) 智能合约废止后，应在区块链网络中保存被终止版本的智能合约代码；
c) 在管理智能合约运行过程中，增强防护要求能有效保障合约免受恶意攻击。

6.4.3.5 合约安全防范

a) 应有相应机制保证系统能对抗由智能合约引起的 DDoS 攻击，防止其长时间占用资源；
b) 应有相应机制保障在系统遭受 DDoS 攻击、服务受到影响时，智能合约的运行可被干预；
c) 应有相应机制防止隔离执行环境中的智能合约访问其执行环境之外的资源。

6.5 钱包技术

6.5.1 安全服务功能

6.5.1.1 钱包认证安全

a) 钱包认证过程中必须设置钱包解锁密码用于解锁钱包，钱包交易密码用于发起交易，钱包日志密码用于浏览钱包日志；
b) 用户使用钱包必须设置解锁密码，用户必须设置解锁密码才能够使用钱包，防止设备丢失后钱包信息被窃取；
c) 用户使用钱包进行交易签名必须设置支付密码，用户需设置支付密码，防止解锁后解密的私钥被窃取；
d) 用户使用钱包日志功能必须设置日志密码，防止钱包密码丢失后攻击者直接清除钱包操作日志；
e) 密码的强度必须达到要求，用户设置的密码强度必须达到要求，防止弱密码被暴力破解；
f) 交易密码需使用多因素认证，用户设置的交易密码需使用多因素认证，例如：指纹、面部识别、OTP 令牌、短信验证码等，防止密码泄露导致私钥丢失；
g) 钱包程序退出后必须重新解锁，防止未授权用户使用钱包；
h) 认证机制必须有防止暴力破解的措施，即设置验证失败重试次数，超过验证次数则停用一段时间并记录相关日志。

6.5.1.2 钱包生成安全

a) 助记词必须通过随机的方法生成，生成的助记词为 12 个及以上，防止助记词数量过少被黑客采用暴力破解的方式进行攻击；
b) 助记词展示界面不允许进行截图操作，防止恶意程序进行截图获取助记词；
c) 私钥生成完成后需立即清除内存中的数据；防止恶意程序通过读取内存中数据盗取私钥；
d) 生成私钥后需让用户重新输入助记词，验证是否记录正确，防止助记词遗忘导致钱包私钥丢失。

6.5.1.3 钱包交易安全

a) 钱包发出的所有交易必须进行签名，确保发出交易的不可被抵赖；
b) 进行交易签名时必须通过输入支付密码解密私钥；
c) 交易签名必须离线生成，签名过程不接触网络；
d) 交易签名生成后必须清除内存中解密后的私钥，防止内存中的私钥被窃取而泄漏；
e) 进行交易时，能够检测生成的交易数据是否被篡改，防止黑客通过篡改交易数据进行攻击。

6.5.1.4 钱包运行环境安全

a) 钱包能够对操作系统进行已知重大漏洞进行检测，使得钱包能运行在安全的操作系统上；
b) 钱包能检测系统是否为虚拟机，手机端需有 root 检测功能；
c) 钱包需具有第三方程序劫持检测功能，防止第三方程序劫持钱包盗取相关用户信息；
d) 钱包能检测针对软件钱包进行的攻击，防止恶意软件攻击钱包，窃取用户信息；
e) 钱包能进行自检完整完整性校验，保证软件的完整性。

6.5.1.5 钱包接口安全

a) 钱包节点应能对连接用户进行用户身份认证，防止未授权操作；
b) 接口需要对数据进行签名，防止黑客对数据被篡改；
c) 接口访问需要添加 token 认证机制，防止黑客进行重放攻击；
d) 节点接口需要对用户连接速率进行限制，防止黑客模拟用户操作进行 CC 攻击。

6.5.1.6 钱包审计安全

a) 钱包节点应能记录用户的连接记录；
b) 钱包节点应能记录用户的交易记录；
c) 能够对节点发生的所有事件进行审计，包括操作记录和日志等；
d) 应能够保存审计记录的过程和结果，便于管理员进行查询；
e) 节点应能定时清除审计记录防止泄密。

6.5.2 安全运行管理

6.5.2.1 钱包测试与加固

a) 钱包必须经过源代码安全测试，防止源代码中的错误写法导致钱包出现安全漏洞；
b) 钱包必须经过渗透测试，测试钱包接口，钱包软件本身，钱包节点等；
c) 钱包引用的第三方库必须经过安全审计，防止第三方库的漏洞影响钱包自身的安全性；
d) 钱包应进行代码加固，防止黑客利用反编译得到源代码从而得到本地加密算法。

6.5.2.2 钱包文档安全

a) 钱包必须包含使用说明及帮助文件，解释和说明软件钱包的功能和使用方法；
b) 钱包必须包含安全建议，指导用户安全的使用钱包；
c) 开发者应对不同版本的程序应提供唯一的版本号；
d) 文档应与软件一一对应，软件更新时，文档版本号应与程序版本号同时更新。

6.6 联盟链技术

6.6.1 基础设施安全

6.6.1.1 网络安全

a) 应根据联盟链具体的运行环境，相应的对节点进行加密防护；
b) 应使用链路加密保护节点之间链路信息安全；
c) 应使用节点加密保护节点之间的传输链路安全；
d) 应使用端点加密保护端点之间的数据安全；
e) 通过 P2P 技术来实现分布式网络机制，各个网络节点之间互不影响或影响很小。

6.6.1.2 代码安全

a) 根据现有开发环境，选择合适的代码进行编写；
b) 可选择沿用主流的编程语言，并进行统一规范地改进；
c) 可选择其他编程语言为基础，加以其他编程模块，遵循相关编程规范。

6.6.1.3 硬件安全

a) 采用专业的硬件设施，保证联盟链的正常运行；
b) 应有完好的硬件机器，保证硬件环境的安全性；
c) 处理重要隐秘信息，所使用硬件应具有应对物理侧信道攻击的能力，防止被窃取重要信息。

6.6.2 安全服务功能

6.6.2.1 身份认证

a) 应使用数字签名算法来检验数据，保证数据的完整性、发送者身份的真实性，防止交易中的抵赖现象；
b) 在数据传输之前，应使用加密算法来对重要隐私信息进行保护。

6.6.2.2 共识机制安全

a) 容错性

共识机制应考虑恶意结点产生的错误，包括发生物理设备以及网络设施的错误，一些主流算法可以容忍小部分拜占庭错误；

b) 一致性

共识机制可以按需求实现不同程度的一致性，包括强一致性和弱一致性；

c) 合法性

用户进行的交易都能被正确的结点确认，且能读取联盟链中正确的数据；

d) 抗攻击

应具有一定的抗攻击能力，在共识过程中发生异常，应能够在异常恢复后能保证数据的安全恢复，可以及时正常地参与共识过程。

6.6.2.3 个人隐私安全

a) 应对存储个人信息以及网络密钥的服务器采取安全防护措施，防止服务器异常时泄露个人信息；
b) 应对用户的隐私和个人数据进行加密保护，确保用户的信息安全，使用对称加密算法防止数据泄露，如可以使用数字签名、哈希等加密算法防止数据被篡改。

6.6.3 安全运行管理

a) 定期对共识机制的安全性进行监测，对所有参与共识过程的节点信息进行审计，保证共识机制能正常的运行；
b) 应在节点相互传输之间采用审计追踪机制，建立完善的日志记录，包含网络传输中的各种详细的信息，防止网络在受到攻击后无法恢复原状态。

6.7 分布式存储技术

6.7.1 基础设施安全

6.7.1.1 操作系统安全

a) 操作系统在运行过程中需要考虑防止黑客利用利用漏洞来提权，应具备强制访问控制机制，实现对系统资源的最小化访问控制；
b) 应能够根据业务架构进行进程的分拆，只对关键核心进程保留高权限，其他无需高权限的进程仅保留满足业务需求的最低权限。

6.7.1.2 芯片安全

a) 应保证系统本身安全可信，能够抵御侧信道攻击、故障注入攻击和芯片级的后门与硬件木马；
b) 具备基于芯片的安全技术，自下而上的保障如固件、操作系统、软件等系统其它部分的安全。

6.7.2 安全服务功能

6.7.2.1 可信启动

a) 安全的数据服务系统基于硬件可信根，构建信任链，对系统进行完整性的度量，保证系统不被篡改；
b) 启动过程为链式关系，逐级进行签名校验，任何一级校验不过就视为启动出错；
c) 启动链完整性可以延伸到系统启动后的一些关键高权限应用， 确保系统运行时具备基础的安全环境。

6.7.2.2 认证和访问控制

a) 任何对数据的相关操作或者对访问数据的软硬件操作请求都必须经过认证，以确定其身份的合法性，进而通过访问控制来确定数据访问者有足够的权限；
b) 根据不同的访问控制策略，针对用户对数据安全访问服务的多样性，结合数据生命周期访问需求和特点，可以采用基于角色访问控制或者基于属性访问控制等方案来实现

数据有效的管控。

6.7.2.3 隐私保护

a) 通过隐私保护算法、有隐私计算、安全计算、零知识证明、可信执行环境、门限签名等技术来保证区块链隐私安全；
b) 防止数据的处理方或接收方因意外或有意的窃取敏感数据，同时又可以保证相关的业务处理不受影响。

6.7.3 安全审计

6.7.3.1 数据传输阶段

a) 数据传输的安全审计需要重点关注传输安全策略的执行情况，对发送方和接收方的设备、接口、通讯协议以及加密方法等信息进行记录，及时发现传输过程中可能引发的敏感数据泄露事件；
b) 通过数据传输双方的日志信息可以发现异常传输的行为。

6.7.3.2 数据存储阶段

a) 数据存储阶段的安全审计主要是对数据存储和读取的动作以及备份的行为进行审计；
b) 通过对数据操作主体、时间、操作类型的分析，发现数据访问者的可能异常行为并确保数据配套的存储安全策略得到正确的执行。

6.7.3.3 数据处理阶段

a) 数据处理阶段的安全审计是对数据处理各个业务接口的操作记录进行审计，发现数据处理当中的风险；
b) 对敏感数据脱敏相关操作的记录进行审计，发现机密信息或者个人数据隐私可能泄露的情况。

6.7.3.4 数据交换阶段

a) 对高价值的数据的导入、导出、共享操作进行持续监控；
b) 追溯交换数据是否已经脱敏，是否已经加密，或者保留有水印等。

6.7.3.5 数据销毁阶段

a) 对存储介质和数据的访问行为、数据销毁过程进行监控；
b) 审计信息应包括数据删除的操作时间、操作人、销毁的方法、数据类型，操作结果等相关信息。

6.7.4 安全运行管理

6.7.4.1 环境安全

a) 数据中心机房只有授权人员才可以进入，其他公司技术和管理人员获得邀请并登记后也可以进入数据中心；
b) 离开数据中心前应确保关闭机柜门、整理好有关设备、离开时必须关闭数据中心大门；
c) 进入数据中心操作时应穿防静电鞋套，保持服装整洁，以防带入灰尘；
d) 进入数据中心后应关闭大门，以免灰尘飘入数据中心；
e) 数据中心内禁止饮食、吸烟，禁止带入不相关的东西；
f) 数据中心专用工具及软件应由系统管理员统一注册、并统一保管，外借工具应登记（借出、借入方均需签名）并应在两工作天内归还，借出者负责跟进收回工具；
g) 系统管理员必须定期检查所有设备是否工作正常，包括检查网络是否畅通、散热设备是否运转、设备是否过热及服务器状态是否良好等等，一般可定一星期检查一次。

6.7.4.2 软件安全

a) 控制系统操作人员权限，数据库及应用系统超级管理员权限只能赋予数据中心内部人员，开发运维商只能赋予普通用户权限，开发运维商如需登录数据库或应用系统时须在数据中心内部人员的陪同下进行；
b) 更新/维护设备或软件时，必须至少提前一天通知受影响用户，紧急情况时应尽量将影响程度降至最低；
c) 按需求安装软件时，必须在其它机器中测试并验证可用后，才可以在服务器中安装；
d) 服务器中软件均为正版软件，禁止在服务器中安装没有授权证（License）的软件，不应在服务器中安装测试版软件。

附 录 A

（规范性）

保障网络信息系统安全的必要条件

保障网络信息系统安全的必要条件，包括但不限于表 A.1 的内容。

表 A.1 保障网络信息系统安全的必要条件（以国家标准为例）

序号	标准号及年代号	标准名称
1	GB 17859-1999	计算机信息系统 安全保护等级划分准则
2	GB/T 20269-2006	信息安全技术 信息系统安全管理要求
3	GB/T 20271-2006	信息安全技术 信息系统通用安全技术要求
4	GB/T 20272-2006	信息安全技术 操作系统安全技术要求
5	GB/T 20273-2019	信息安全技术 数据库管理系统安全技术要求
6	GB/T 20282-2006	信息安全技术 信息系统安全工程管理要求
7	GB/T 20984-2007	信息安全技术 信息安全风险评估规范
8	GB/T 20985.1-2017	（采）信息技术 安全技术 信息安全事件管理 第 1 部分：事件管理原理
9	GB/T 20985.2-2020	（采）信息技术 安全技术 信息安全事件管理 第 2 部分：事件响应规划和准备指南
10	GB/T 20988-2007	信息安全技术 信息系统灾难恢复规范
11	GB/T 21052-2007	信息安全技术 信息系统物理安全技术要求
12	GB/T 22239-2019	信息安全技术 网络安全等级保护基本要求
13	GB/T 22240-2020	信息安全技术 网络安全等级保护定级指南
14	GB/T 25058-2019	信息安全技术 网络安全等级保护实施指南
15	GB/T 25070-2019	信息安全技术 网络安全等级保护安全设计技术要求
16	GB/T 28448-2019	信息安全技术 网络安全等级保护测评要求
17	GB/T 28449-2018	信息安全技术 网络安全等级保护测评过程指南
18	GB/T 32915-2016	信息安全技术 二元序列随机性检测方法
19	GB/T 35293-2017	信息技术 云计算 虚拟机管理通用要求

附 录 B

（规范性）

保障密码技术安全的必要条件

保障密码技术应用安全的必要条件，包括但不限于表 B.1 的内容。

表 B.1 保障密码技术应用安全的必要条件（以国家标准为例）

序号	标准号及年代号	标准名称
1	GB/T 17901.1-2020	信息技术 安全技术 密钥管理 第 1 部分：框架
2	GB/T 20518-2018	信息安全技术 公钥基础设施 数字证书格式
3	GB/T 32905-2016	信息安全技术 SM3 密码杂凑算法
4	GB/T 32907-2016	信息安全技术 SM4 分组密码算法
5	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
6	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
7	GB/T 32918.4-2016	信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分：公钥加密算法
8	GB/T 33560-2017	信息安全技术 密码应用标识规范
9	GB/T 37092-2018	信息安全技术 密码模块安全要求
10	GB/T 38540-2020	信息安全技术 安全电子签章密码技术规范
11	GB/T 38625-2020	信息安全技术 密码模块安全检测要求
12	GB/T 38635.2-2020	信息安全技术 SM9 标识密码算法 第 2 部分：算法
13	GB/T 39786-2021	信息安全技术 信息系统密码应用基本要求

附 录 C
（资料性）
关键服务的相关内容

C.1 关键服务的内涵

C.1.1 关键服务的特征

基于区块链技术的关键服务具有以下特征：

a) 去中心化

区块链是由众多节点共同组成的点对点网状结构，没有第三方管理，通过分布式记录和存储的形式，各个节点之间实现数据信息的验证、传递和管理。数据在每个节点互相备份，各节点地位平等共同维护系统功能，因此系统不会因为任意节点的损坏或异常而影响正常运行，使得基于区块链的数据存储具有较高的安全可靠性。

b) 可溯源性

区块链中的数据信息存储在带有时间戳的链式区块结构里，具有极强的可追溯性和可验证性。区块链中任意两个区块间都通过密码学方法相关联，可以追溯到任何一个区块的数据信息。

c) 共识机制

共识机制主要指网络中的所有节点间如何达成共识的认证原则，去认定一份交易信息的有效性，保证信息的真实可靠。共识机制可以减少伪冒交易的发生，只有超过 51%的节点成员达成共识，数据交易才能发生，可以保证交易信息的一致性。

d) 高度信任

在区块链技术应用中任何恶意欺骗的行为都会遭到其他节点的排斥。区块链技术具有开源、透明的特性，任意节点间的数据交换通过数字签名技术进行验证，按照系统既定的规则运行，保证数据信任。

C.1.2 关键服务的应用载体与形式

a) 传统的应用载体与形式有互联网站、应用程序等；传统载体技术虽然较为成熟，但是开发、搭建一套区块链技术应用并非容易，资源的缺乏、底层平台搭建的复杂及运维的烦琐，使得企业无法聚焦于上层应用的创新。

b) 新型应用载体与形式以云服务平台为主，云的开放性和云资源的易获得性，使得云平台成为当前区块链创新的最佳载体，云基础设施和云平台服务可以提升运营效率和降低投入门槛。

C.2 关键服务的场景

C.2.1 公共服务的领域

a) 身份验证

区块链技术可以将所有与个人证明有关的信息统一存储，比如身份信息、出生证结婚证等，这样可以免除了许多繁琐的认证步骤以及避免一些安全风险。

b) 公共资产的可追踪

将区块链技术应用于公共资产管理方面，可以有效地实现资产公开化、透明化。

c) 社会福利管理

将社会福利写入区块链中，通过时间戳来确保数据精度，这些记录完全无法被篡改，可以有效避免社会福利欺诈问题。

C.2.2 交通领域

a) 个人交通出行服务

通过区块链技术可以掌握乘客、司机、车辆等数据信息，实现车辆行程和司机履历的可追

溯，可以实时获取车辆的具体位置，一旦遇到紧急情况，执法管理部门可以通过信息区块快速掌握到具体的信息，有效地解决问题，提升用户的出行体验。

b) 车辆道路高效管理

城市交通的管理，是城市治理的基本要求。传统管理方式需要消耗大量资源且效率较低，使用区块链技术可以将交通领域的监控系统智能化，利用区块链技术，建立道路信息、市民出行、车流等数据，实现各部分数据的共享，可以实时掌握道路的具体情况，统筹城市交通信号进行精准分析，有效提高城市交通管理的能力。

c) 交通物流信息溯源

传统的溯源技术存在着信任成本，可以应用区块链技术来解决产品运输、流通等环节的不透明问题，共识机制确保了数据的一致性并且不可篡改。

C.2.3 金融领域

a) 证券交易

区块链应用在证券发行和交易中，可以实现去中介的P2P交易模式，对证券发行机构和客户进行匹配自动达成智能合约，节省费时费力的中间环节，交易信息存储在区块链中可以保证安全性与透明性。

b) 智能理赔

利用区块链技术将保险产品信息从投保到理赔的全过程进行整合写入区块链，实现了全流程追溯和各机构的信任共享。

c) 数字货币

区块链应用在数字货币中，其所具备的去中心化信任机制，可以提升账户之间经济运行速率，并且可以针对反洗钱、反逃税、反腐败等违法犯罪活动进行资金流信息的追踪与管控。

C.2.4 能源领域

a) 能源交易

我国能源市场呈现开放程度小、规模小、分散式的特点，运用传统管理方式会消耗过多的资源，且不具有实时性。而区块链技术所具有的去中心化、公开透明、不可篡改和可追溯的特点可以很好地满足当前能源市场交易的需求。

b) 能源消费

基于区块链分布式账本与智能合约的特征，实现能源消费侧和供给侧的公开透明。应用场景包括水电供给等公用设施的资源管理、供应链管理、电动汽车充放电智能支付系统等。

c) 能源供给

基于区块链去中心化特征，可以实现信息实时共享，避免多种能源的重复建设，减小能源供给系统的浪费。

参考文献

[1] 国家发展改革委会等.《加快培育新型消费实施方案》.2021
[2] 国务院办公厅.《关于以新业态新模式引领新型消费加快发展的意见》.2020
[3] 中共中央政治局.《国家安全战略（2021—2025年）》.2021
[4] 龚刚军,杨晟,王慧娟等.综合能源服务区块链的网络架构、交互模型与信用评价[N].中国电机工程学报,2020-9-20(18)
[5] 颜有起.论区块链技术在交通领域的应用[J].现代传输,2021(05):59-61
[6] 王波,王轶玮.区块链金融：场景运用、风险挑战与法律监管[J].西部金融,2021(07):54-58
[7] DB61/T 1283-2019 区块链安全测评 指标体系