ICS 35.080
L 77

DB31

上 海 市 地 方 标 准

DB31/T XXXX-2020

区块链技术安全通用规范

General Specification of Blockchain Technology Security

20XX－XX－XX 发布　　20XX－XX－XX 实施

上海市质量技术监督局　发布

目次

前　言

本标准按照 GB/T 1.1-2009 给出的规则起草。

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这些专利的责任。

本标准由上海市市场监管局提出并归口。

本标准主要起草单位：

本标准主要起草人：

引　言

我国已明确要求把区块链作为核心技术和自主创新的重要突破口，加快推动区块链技术和产业创新发展。在区块链技术和产业应用快速发展阶段，迫切需要关注区块链技术应用中存在的、潜在的安全隐患。本规范在 T/SSIA 0002-2018 的基础上，进一步聚焦、细化区块链技术的共性技术风险，提出对应的安全通用要求，对于促进区块链技术健康发展和保障区块链技术的安全应用具有十分重要的意义。

基于三层区块链技术构架，本规范逐层分析安全风险并提出相应的技术安全要求。同时，按照适度保护原则，本规范将通用“应”、“宜”等用词，区分基本要求和增强要求，以满足不同区块链应用的安全需求。

本规范共分为 9 个章节。第 6 章至第 8 章分析了区块链安全风险并给出了安全措施，第 9 章阐述了实现区块链安全的相关要求。附录 A 是资料性附录，给出了本规范具体安全要求适用的区块链类型。

区块链技术安全通用规范

1 范围

本规范适用于基于区块链技术的产品、应用的安全设计、开发、维护及测试等。

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 22239-2019 信息系统安全等级保护基本要求

GB/T 18336-2015 信息技术安全评估准则

GB/T 35273-2020 个人信息安全规范

T/SSIA 0002-2018区块链技术安全通用规范

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。

3.1

区块链 blockchain

是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构，并通过密码学等方式保证数据不可篡改和不可伪造的去中心化的互联网公开账本。

3.2

共识机制 consensus mechanism

指形成共同认识或达成一致意见的运作方式、方法和规则。区块链共识机制保证了以去中心化方式维护分布式数据库数据的一致性。区块链中常用的共识机制主要包括：工作量证明机制、权益证明机制、股份授权证明机制和验证池机制等。

3.3

共识算法 consensus algorithms

用于保证系统中不同节点数据在不同程度下的一致性和正确性的算法。根据区块链类型的不同划分，共识算法主要可以分为两大类。一类是用于公链场景的共识算法，主要包括工作量证明算法POW、股权证明算法POS和委托权益证明算法DPOS。另外一类是用于联盟链场景的共识算法，主要包括拜占庭容错算法PBFT和RAFT等。

3.4

时间戳 time stamp

是一个字符序列，唯一地标识某一刻的时间点。区块链中的时间戳，是某一时间内发生的所有事件在区块链数据库中进行唯一的、不可更改的记录。

3.5

哈希算法 hash

即哈希函数。它是一种单向密码体制，是一个从明文到密文的不可逆的映射，只有加密过程，没有解密过程。

3.6

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密、数字签名和登录认证等。区块链系统中，涉及到非对称加密算法主要有RSA、D-H、ECC（椭圆曲线加密算法）等。

3.7

智能合约 smart contracts

由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的一段计算机代码，是现实世界中合约和规则的算法实现。

3.8

P2P 网络技术 P2P network technology

又被称为点对点网络技术，是区块链系统中连接各对等节点的组网技术。

3.9

联盟链 consortium blockchain

区块链由多个中心控制，系统由几个权威的机构共同分布式记账，这些节点再根据共识机制协调工作。

3.10

私有链 private blockchain

区块链由某个组织或机构控制，参与节点的资格会有严格的限制。

4 缩略语

下列缩略语适用于本文件。

DDoS：分布式拒绝服务（Distributed Denial of Service）

DoS：拒绝服务（Denial of Service）

DNS：域名系统（Domain Name System）

ECC：椭圆曲线密码学（Elliptic Curve Cryptography）

CAP：一致性（Consistency）、可用性（Availablity）、分区容错性（Partition）

API: 应用程序接口（Application Programming Interface）

IPSec：Internet协议安全性（Internet Protocol Security）

TLS：传输层安全性协议（Transport Layer Security）

5 区块链技术架构

为了便于分析，结合最佳实践和已知区块链风险分布情况，本规范提出区块链技术的三

层技术架构。如图 1 所示。

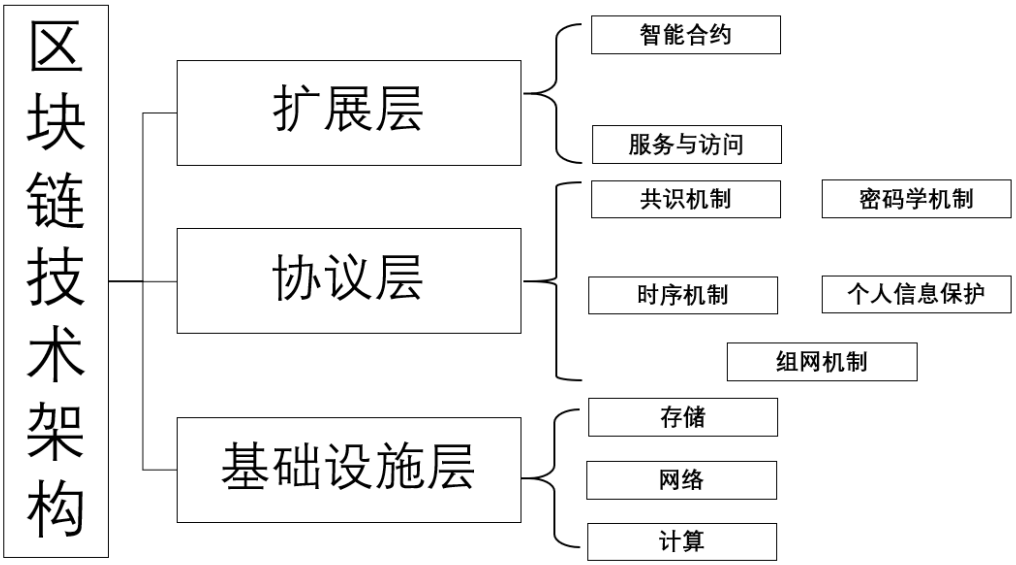

图 1 区块链技术架构

其中，基础设施层将传统网络安全与区块链安全联系起来，协议层基于基础设施层提供的硬件或网络基础体系实现相应功能，并为扩展层提供相应功能支持服务；协议层包含区块链技术的几大关键机制：共识机制、密码学机制、时序机制以及组网机制，协议层向下连接基础设施层，向上衔接扩展层。扩展层通过调用协议层功能组件，可以提供多元化的服务和访问。

需要指出的是，区块链应用安全也是区块链安全不可忽视的关键环节。目前，区块链已经广泛应用在数字金融、物联网、智能制造、供应链管理等诸多领域。不同行业应用安全需求差别较大，本规范聚焦于区块链自身的技术通用性安全，重点分析区块链核心机制内在安全缺陷以及部署应用过程中可能引发的安全风险。因此，不再将应用层安全纳入技术架构体系。区块链应用安全要求可参考《GB/T 22239-2019 信息系统安全等级保护基本要求》选择合适等级实施安全保护。

6 基础设施层安全风险及安全措施

6.1 风险分析

6.1.1 存储

区块链存储面临的安全风险包括来自物理环境的安全风险以及来自存储设备和存储机制的安全风险，安全风险包括但不限于：

1） 来自物理环境的安全风险

a） 区块链节点部署的物理环境存在安全风险；

b） 存放存储设备的物理运行环境存在安全风险。

2） 来自存储设备和存储机制的安全风险

a） 数据库中可能存在未及时修复的安全漏洞，导致未经授权的区块链的设备访问和入侵；

b） 区块链相关设备存在软硬件漏洞，例如区块链相关的硬件加密设备，如硬件钱包，存在安全漏洞，不符合相关安全规范；

c） 数据容量达到存储上限无法同步账本。

6.1.2 网络环境

基础设施层为区块链系统的运行提供传统的网络环境，存在安全风险包括但不限于：

a） DDoS 攻击；

b） 病毒木马攻击；

c） DNS 污染；

d） 路由广播劫持。

6.1.3 计算环境

基础设施层为区块链系统的运行提供计算环境，存在数据丢失和泄露的安全风险以及数据不合规的安全风险，安全风险包括但不限于：

1） 数据丢失和泄露

a） 针对区块数据和数据文件的窃取、破坏导致的数据丢失和泄露；

b） 因误操作、系统故障、管理不善等问题导致的数据丢失和泄露；

c） 因网络断裂或恶意数据攻击导致的链上与链下分布式存储数据不一致的风险。

2） 数据不合规

区块链数据难以篡改的特性使得上链数据很难通过传统的方式修改和删除，一旦有害信息或者威胁用户隐私的数据上链将会带来不可撤销的危害和损失，因而存在数据不合规的安全风险以及恶意信息攻击风险。

6.2 安全措施

层面		安全风险	安全措施
基础设施层	存储	区块链节点部署的物理环境存在安全风险	1、节点部署的物理环境，应根据 GB/T 22239-2019 规范中给出的 3 级物理安全要求，结合区块链系统存储的数据性质，做出妥善安排； 2、使用符合国家相关安全规范的区块链硬件加密设备； 3、保证部署节点的硬件设备存储容量可扩展。
		存放存储设备的物理运行环境存在安全风险	
		数据库中可能存在未及时修复的安全漏洞	
		区块链相关设备存在软硬件漏洞	
		数据容量达到存储上限无法同步账本	
	网络	DDoS 攻击	1、提供网络隔离措施，确保服务器的安全； 2、通过部署资源监控和入侵检测等防范机制，对网络资源使用情况、网络运行情况进行监测分析，实现对恶意节点、DDoS 等入侵攻击的有效检测和联动处置。
		病毒木马攻击	
		DNS 污染	
		路由广播劫持	
	计算	数据丢失和泄露的安全风险	1、采取技术措施保障计算环境的安全可靠； 2、采用核心节点冗余配置，保障在断网断线情况下的业务可用性； 3、监视节点的 CPU、硬盘、内存、网络等资源的使用情况，遇到节点硬件与网络异常，应及时报警并
		数据不合规的安全风险	

			处置； 4、区块链系统存储涉及金融与个人隐私等敏感信息时，要做加密处理； 5、加强对上链数据内容的过滤审查，防止因为区块链的不可篡改性造成的不可撤销的损失。

7 协议层安全风险及安全措施

协议层包含区块链的几大关键机制：共识机制、密码学机制、组网机制等，分析协议层的安全风险，需要综合考虑区块链技术自身的设计漏洞、常见的攻击方式、现有的安全防护措施等因素。

7.1 风险分析

7.1.1 共识机制

共识机制是区块链技术框架的核心，共识算法的作用是使数据保持一致性。可以从一致性、容错性和安全攻击三个维度分析共识机制的安全风险。共识机制的安全风险包括：由共识机制自身设计漏洞导致的安全风险和实际应用场景下的共识安全风险，安全风险包括但不限于：

1） 由共识机制自身设计漏洞导致的安全风险

a） 根据 CAP 准则，一个分布式系统最多只能同时满足一致性、可用性和分区容错性中的两条，因而共识机制可能面临可用性和一致性的选择，当节点或网络连接失效时，可能存在共识无法收敛、收敛时间较长超出可用范围、记录分叉等安全风险；

b） 当攻击者算力或比例达到一定比例时，存在恶意节点控制共识进程的安全风险；

c） 攻击者采用双花攻击、自私挖矿攻击、短程攻击、长程攻击、币龄堆积、预计算攻击、女巫攻击等攻击方式，达到双重支付、回滚记录、获得网络控制权等攻击目的。

2） 实际应用场景下的共识安全风险

a） 在联盟链的场景下，联盟参与者和节点数较少，联盟成员可进行密谋，从而绕过共识机制的限制，任意修改链上数据；

b） 不同的场景对安全性、扩展性、性能效率的需求不同，因共识算法选择不当可能导致安全风险。

7.1.2 密码学机制

密码学机制是保证区块链安全的关键，可从密码算法自身设计、密钥管理以及量子计算的发展等维度分析密码学机制面临的安全风险。密码学机制面临的安全风险包括来自密码算法的安全风险、来自密钥的安全风险以及来自量子计算机的安全风险，安全风险包括但不限于：

1） 来自密码算法的安全风险

a） 密码算法自身设计存在安全风险，如哈希算法面临碰撞威胁；

b） 密码算法开发实现中存在后门和漏洞，如利用 RSA-1024 滑动窗口机制中泄露的信息可完全恢复密钥。

2） 来自密钥的安全风险

a） 密钥生成、分发、存储过程中因人员操作或管理不当带来的安全风险，包括密钥丢失被盗等。

3）来自量子计算机的安全风险

a） 随着量子计算技术的发展，非对称加密算法中的大数因子分解问题存在秒级时间内被破解的风险。

7.1.3 时序机制

区块链时序机制面临的安全风险包括但不限于：

a） 区块链节点未做时间同步，或时间同步过程被非法入侵，造成节点同步时间超过区块链共识协议的允许误差范围；

b） 时间戳不可信。

7.1.4 个人信息保护

区块链的个人信息保护是指通过密码学手段，保障用户身份及交易内容等个人信息安全。个人信息保护面临的安全风险包括身份信息泄露的安全风险和交易信息泄露的安全风险，安全风险包括但不限于：

1） 身份信息泄露的安全风险

a） 用户的身份信息、物理地址、IP 地址与区块链上的用户公钥、地址等公开信息之间存在关联关系。

2） 交易信息泄露的安全风险

a） 攻击者通过关联分析，可以推测出交易数据背后有价值的敏感信息；

b） 未授权节点访问交易数据。

7.1.5 组网机制

P2P 网络为对等网络环境中的节点提供一种分布式、自组织的连接模式，P2P 组网机制面临的安全风险包括由 P2P 技术缺陷带来的安全风险和由设备故障导致的安全风险，安全风险包括但不限于：

1） 由 P2P 技术缺陷带来的安全风险

a） P2P 网络节点准入要求极低，与专业服务器相比安全漏洞多防护差，黑客很容易针对少量关键节点发起网络路由攻击或者直接入侵，通过日蚀攻击获得利益；

b） 攻击者针对 P2P 网络缺少身份认证、数据验证、网络安全管理等机制的不足，发布非法内容,传播蠕虫、木马、病毒,实施 DDoS 攻击、路由攻击等。

2） 由设备故障导致的安全风险

a） 因节点故障、网络连接断裂带来的组网安全风险，导致数据不一致性、拒绝服务、节点隔离等。

7.2 安全措施

层面	安全风险		安全措施
协议层	共识机制	由共识机制自身设计漏洞导致的安全风险	1、 加强共识协议在容错性上的设计，使得其可以容忍一定范围的节点物理或网络故障导致的非恶意节点断线和网络分区，并且能够抵御合谋攻击、女巫攻击等恶意攻击行为； 2、 确保多个节点参与共识和确认，防止任何独立节点的恶意操作； 3、 通过引入链外可信第三方的方式来增强联盟链的数据不可篡改性；
		实际应用场景下的共识安全风险	

			4、 根据网络规模、参与方数量、交易吞吐量等需求调整算法规模。
	密码学机制	来自密码算法的安全风险 来自密钥的安全风险 来自量子计算机的安全风险	1、使用符合密码相关国家要求的安全可靠的密码机制，密码实现过程中进行有效的代码混淆； 2、使用有效的密钥管理技术； 3、使用抗量子攻击的密码机制。
	时序机制	区块链节点未做时间同步，或时间同步过程被非法入侵	1、采用技术措施保证账本记录的时序一致性； 2、使用由第三方时间戳服务机构产生的时间戳，保证时间戳可信性。
	个人信息保护	身份信息泄露的安全风险 交易信息泄露的安全风险	1、使用主流的签名方式来保证消息的隐私，包括但不限于盲签名、环签名、群签名等； 2、采用侧链技术实现个人信息保护功能，将用户业务敏感数据放到侧链上，而不存储在公开的主链上等； 3、对账本进行隔离，让账本只在参与共同记账的组织之间共享，而其他组织无权访问账本。
	组网机制	由 P2P 技术缺陷带来的安全风险 由设备故障导致的安全风险	1、采取技术措施保证数据传输的保密性、完整性和可靠性等； 2、在节点与节点之间建立安全的信息传输通道； 3、采用核心节点冗余配置，保障在断网断线情况下的业务可用性； 4、采用技术手段保证各节点的账户记录的一致性； 5、对信息进行过滤审计，防止因为区块链的不可篡改性造成的不可撤销的损失。

8 扩展层安全风险及安全措施

8.1 风险分析

8.1.1 智能合约

智能合约以代码的形式实现业务逻辑,智能合约的安全风险包括合约内容的安全风险以及合约运行的安全风险，安全风险包括但不限于：

1） 合约内容的安全风险

a） 编译语言不成熟，直接危害智能合约的执行和用户的个人数字资产；

b） 合约代码存在漏洞，导致交易依赖攻击、时间戳依赖攻击、调用深度攻击、可重入攻击、整数溢出攻击等安全风险；

c） 合约内容不符合相关法律规范。

2） 合约运行的安全风险

a） 智能合约的运行环境没有与外部隔离，导致系统遭受攻击；

b） 智能合约在调用时会涉及到类型匹配、Gas 限制、堆栈限制以及调用逻辑等问题，恶意攻击者能够在调用时利用代码或者逻辑上的漏洞，对合约进行攻击；

c） 智能合约访问外部数据时,不能保证不同节点访问的数据的一致性与真实性，也无法避免数据提供网站恶意变更数据或被攻击引起单点失效问题。

8.1.2 服务与访问

通过 API 接口，区块链可以提供多元化的服务和访问。区块链的服务与访问面临的主要安全风险包括由权限控制管理问题导致的安全风险和区块链自身机制和开源软件导致的安全风险，安全风险包括但不限于：

1) 由权限控制管理问题导致的安全风险
   a) 非法用户接入。如，未被标识用户从接口接入；
   b）非授权访问。如，非法用户进入网络或系统进行违法操作和合法用户以未授权的方式进行操作。
2) 由区块链自身机制和开源软件导致的安全风险
   a) 缺乏安全管理机构及监管审计机构参与管控区块链系统。区块链追求去中心化的设计，使得监管部门难以准确定位主体，从而出现监管盲区，导致数据泄露、隐私侵犯、恐怖融资等问题；
   b) 开源区块链软件因开发问题引发输入验证、API 误用、内存管理等安全漏洞。

8.2 安全措施

层面	安全风险		安全措施
扩展层	智能合约	编译语言不成熟	1、 智能合约编写过程中应使用最新的安全规范，并进行代码安全审查； 2、 在智能合约运行环境中完成代码的执行与动态安全检测； 3、 应提供运行载体，如虚拟机等，应确保虚拟机的安全性，保证智能合约运行环境与外隔离； 4、 对区块链系统服务器进行定期漏洞扫描检查包括但不限于服务器本身的漏洞、区块链账本的漏洞、智能合约的漏洞，并对发现的安全漏洞和隐患提出修复方案进行审批，审批通过后进行修复。 5、 应提供对已知攻击的解决方案，包括竞态、重入、交易顺序依赖等； 6、 限制智能合约的操作权限，避免权限漏洞； 7、 应严格限制外部合约的调用，防止不受信任的外部合约； 8、 提供方案控制智能合约对外部环境的访问，控制隔离执行环境中的智能合约访问其执行环境之外的资源。
		合约代码存在漏洞	
		合约内容不符合相关法律规范	
		智能合约的运行环境没有与外部隔离，导致系统遭受攻击	
		智能合约在调用时会涉及到类型匹配、Gas 限制、堆栈限制以及调用逻辑等问题，恶意攻击者能够在调用时利用代码或者逻辑上的漏洞，对合约进行攻击	
		智能合约访问外部数据时,不能保证不同节点访问的数据的一致性与真实性，也无法避免数据提供网站恶意变更数据或被攻击引起单点失效问题	
	服务与访问	非法用户接入	1、接口应根据业务需求做好权限管理，防止未授权的访问和调用，针对不同的用户配置不同的访问权限； 2、区块链系统设计支持安全管理机构和监管审计机构接入，在遭遇特殊突发事件时，能对区块链系统实施干预。 3、应提供内容监管服务，强化区块链的安全监管。
		非授权访问	
		缺乏安全管理机构及监管审计机构参与管控区块链系统	
		开源区块链软件因开发问题引发输入验证、API 误用、内存管理等安全漏洞	

9 安全要求

安全要求分为总体要求和层面要求。总体要求包括数据安全、共识安全、个人信息保护、智能合约安全和内容安全五个方面；层面要求包括基础设施层安全、协议层安全和扩展层安全。

9.1 总体要求

9.1.1 数据安全

a) 应根据根据业务需求分类设置访问权限，仅允许授权用户对数据进行相应的操作；
b) 应设置认证规则，规定每个节点加入区块链的方式和有效的身份识别方式；
c) 应设置访问控制，规定用户的访问权限；
d) 当受到攻击导致部分功能受损的情况下,区块链系统应具备短时间内修复和重构的能力；
e) 应确保新加入的节点可提供无差别服务；
f) 用户的访问数据请求应在设计要求的时间内得到区块链网络响应。

9.1.2 共识安全

a) 应确保任何已经被记录在区块链上并达成共识的交易都无法更改；
b) 应确保诚实节点提交的合法数据终将由全网节点达成共识并被记录在区块链上。合法数据包括诚实节点提交的合法交易、正确执行的智能合约中间状态变量、结果等。

9.1.3 个人信息保护

个人信息保护是对用户身份信息等用户不愿公开的敏感信息的保护。在区块链中，主要针对用户身份信息和交易信息两部分内容。

个人信息保护的安全要求是采取技术手段保证个人信息生命全周期各环节不被未授权的第三方获取，并保护交易方的身份不被识别和冒用。

9.1.4 智能合约安全

a) 应确保智能合约的文本安全和代码安全；
b) 应确保智能合约在执行过程中出现漏洞甚至被攻击时,不会对节点本地系统设备造成影响，也不会使调用该合约的其他合约或程序执行异常。

9.1.5 内容安全

区块链上传播和存储的信息内容应符合《网络信息内容生态治理规定》要求,保证区块链网络中信息符合法律法规，遵循公序良俗，不损害国家利益、公共利益和他人合法权益。

9.2 基础设施层安全

9.2.1 存储安全

a) 应符合 GB/T 22239-2019 规范中给出的 3 级物理安全相关要求；
b) 应保证部署节点的硬件设备存储容量可扩展，避免因数据容量达到上限而无法同步账本。

9.2.2 网络安全

a) 应符合 GB/T 22239-2019 规范中给出的 3 级安全通信网络相关安全要求；
b) 应符合 GB/T 22239-2019 规范中给出的 3 级安全区域边界相关安全要求；
c) 应具备检测和防御恶意节点的机制，能够检测出网络中的恶意节点，并进行针对性处理。

9.2.3 计算安全

a) 应符合 GB/T 22239-2019 规范中给出的 3 级安全计算环境相关安全要求；
b) 应符合 GB/T 22239-2019 规范中给出的 3 级安全管理中心资源监控的相关安全要求。

9.3 协议层安全

9.3.1 共识机制安全

a) 应使用设计合理和安全的共识机制，并能够有效防范常见的共识攻击；
b) 应确保多个节点参与共识和确认，防止任何独立节点的恶意操作；
c) 应采用技术手段保证各节点的账户记录的一致性；
d) 宜支持多种共识算法并实现共识算法可插拔，可根据需求切换选择共识算法；
e) 宜提供根据网络规模、参与方数量、交易吞吐量等需求调整算法规模的功能。

9.3.2 密码学机制安全

a) 应使用较为安全的哈希算法，如国密算法 SM3、SHA256 等；
b) 应使用非对称加密算法，用于信息加密、数字签名和登录认证等场景；
c) 应具备明确的密钥管理方案；
d) 应使用国际主流的数字签名，如 SM2、RSA、ECC 等；
e) 在重要业务场景，宜使用权威公正的第三方 CA 机构签发的数字证书来进行数字签名和签名验证等相关工作，确保信息的机密性、完整性和不可抵赖性；
f) 使用随机数时，应按照国家密码管理部门的要求生成随机序列。

9.3.3 时序机制

a) 宜采用技术措施保证账本记录的时序一致性；
b) 宜使用由第三方时间戳服务机构产生的时间戳，保证时间戳可信性。

9.3.4 个人信息保护

a) 应使用主流的签名方式来保证消息的隐私，包括但不限于盲签名、环签名、群签名等；
b) 应提供数据变换技术，如数据加密、敏感数据脱敏等手段，可将敏感数据进行变换；
c) 宜采用侧链技术实现个人信息保护功能，将用户业务敏感数据放到侧链上，而不存储在公开的主链上等。

9.3.5 组网机制安全

a) 应提供节点服务器之间的身份认证；
b) 应支持动态加入和删除节点，且不影响业务的正常运行；
c) 应确保节点断线重连后，可与其他节点实现状态一致性；
d) 应在节点与节点之间建立安全的信息传输通道，例如 TLS，Ipsec 等协议；
e) 节点应对区块链网络中提交的相关信息进行有效性验证。

9.4 扩展层安全

9.4.1 智能合约安全

9.4.1.1 智能合约内容安全

a) 智能合约源代码应符合安全编码规范要求，确保智能合约的安全性；
b) 应采用技术手段防止对合约内容的篡改；
c) 智能合约应定义版本号，调用智能合约时应明确记录智能合约版本；
d) 智能合约应具有向后兼容性，智能合约更新升级或重新部署后，新智能合约能兼容或迁移原智能合约数据。

9.4.1.2 智能合约运行安全

a) 应提供智能合约的升级和废止功能，智能合约的升级操作应记录在区块中，符合区块链交易要求、遵从交易执行的流程；
b) 应提供合约安全检测等手段，确保可及时发现和处置出现的问题，降低安全风险；
c) 应提供方案控制智能合约对外部环境的访问，控制隔离执行环境中的智能合约访问其执行环境之外的资源。外部数据的影响范围仅限于智能合约范围内，不应影响区块链系统的整体运行；
d) 当智能合约出现错误时，应提供智能合约挂起功能；
e) 应提供运行载体，如虚拟机等，智能合约应在虚拟机等隔离环境中运行，不能直接运行在参与区块链的节点本地系统上，防止运行智能合约的本地操作系统遭受攻击；
f) 对于与区块链系统外部数据进行交互的智能合约，外部数据的影响范围仅限于智能合约范围内，不应影响区块链系统的整体运行；

g) 应对智能合约的操作权限进行限制，避免权限漏洞；
h) 应严格限制外部合约的调用，防止不受信任的外部合约；
i) 宜提供有效的方案防止智能合约被恶意滥用，如：多次调用无意义操作，从而造成DoS 攻击使区块链系统瘫痪。

9.4.2 服务与访问安全

9.4.2.1 权限控制

a) 接口应根据业务需求做好权限管理，防止未授权的访问和调用，针对不同的用户配置不同的访问权限；
b) 应设置操作限制，防止攻击者通过大量信息堵塞整个区块链；
c) 当支持多链架构时，应保证数据的安全隔离；
d) 应支持区块链节点版本升级，在升级前应在测试环境进行验证，保证升级过程中对业务的平滑过渡；
e) 区块链节点版本应具有后向兼容性，区块链节点升级后仍支持旧版本的数据。

9.4.2.2 审计监管

a) 应提供安全审计功能，对重要操作进行审计；
b) 安全管理机构的所有干预操作行为应被记录实现不可更改并可被查询，做到可审计、可追溯；
c) 应提供内容监管服务，强化区块链的安全监管；
d) 应支持安全管理机构接入，在发生特殊突发事件时，可对区块链系统进行干预。

附录 A

（规范性附录）
安全要求适用情况表

A.1 基础设施层安全

	安全要求	适用区块链类型
存储安全	a) 应符合 GB/T 22239-2019 规范中给出的 3 级物理安全相关要求；	联盟链和私有链
	b) 应保证部署节点的硬件设备存储容量可扩展，避免因数据容量达到上限而无法同步账本。	联盟链和私有链
网络安全	a) 应符合 GB/T 22239-2019 规范中给出的 3 级安全通信网络相关安全要求；	联盟链和私有链
	b) 应符合 GB/T 22239-2019 规范中给出的 3 级安全区域边界相关安全要求；	联盟链和私有链
	c) 应具备检测和防御恶意节点的机制，能够检测出网络中的恶意节点，并进行针对性处理。	联盟链
计算安全	a) 应符合 GB/T 22239-2019 规范中给出的 3 级安全计算环境相关安全要求；	联盟链和私有链
	b) 应符合 GB/T 22239-2019 规范中给出的 3 级安全管理中心相关安全要求。	联盟链和私有链

A.2 协议层安全

	安全要求	适用区块链类型
共识机制安全	a) 应使用设计合理和安全的共识机制，并能够有效防范常见的共识攻击；	联盟链和私有链
	b) 应确保多个节点参与共识和确认，防止任何独立节点的恶意操作；	联盟链
	c) 应采用技术手段保证各节点的账户记录的一致性；	联盟链
	d) 宜支持多种共识算法并实现共识算法可插拔，可根据需求切换选择共识算法；	联盟链和私有链
	e) 宜提供根据网络规模、参与方数量、交易吞吐量等需求调整算法规模的功能。	联盟链和私有链
密码学机制安全	a) 应使用较为安全的哈希算法，如国密算法 SM3、SHA256 等；	联盟链和私有链
	b) 应使用非对称加密算法，用于信息加密、数字签名和登录认证等场景；	联盟链和私有链
	c) 应具备明确的密钥管理方案；	联盟链和私有链
	d) 应使用国际主流的数字签名，如 SM2、RSA、ECC	联盟链和私有链

	等；	
	e) 在重要业务场景，宜使用权威公正的第三方 CA 机构签发的数字证书来进行数字签名和签名验证等相关工作，确保信息的机密性、完整性和不可抵赖性；	联盟链和私有链
	f) 使用随机数时，应按照国家密码管理部门的要求生成随机序列。	联盟链和私有链
时序机制	a) 宜采用技术措施保证账本记录的时序一致性；	联盟链和私有链
	b) 宜使用由第三方时间戳服务机构产生的时间戳，保证时间戳可信性。	联盟链和私有链
个人信息保护	a) 应使用主流的签名方式来保证消息的隐私，包括但不限于盲签名、环签名、群签名等；	联盟链和私有链
	b) 应提供数据变换技术，如数据加密、敏感数据脱敏等手段，可将敏感数据进行变换；	联盟链和私有链
	c) 宜采用侧链技术实现个人信息保护功能，将用户业务敏感数据放到侧链上，而不存储在公开的主链上等；	联盟链
组网机制安全	a) 应提供节点服务器之间的身份认证；	联盟链
	b) 应支持动态加入和删除节点，且不影响业务的正常运行；	联盟链和私有链
	c) 应确保节点断线重连后，可与其他节点实现状态一致性；	联盟链和私有链
	d) 应在节点与节点之间建立安全的信息传输通道，例如 TLS，ipsec 等协议；	联盟链和私有链
	e) 节点应对区块链网络中提交的相关信息进行有效性验证。	联盟链和私有链

A.3 扩展层安全

	安全要求	**适用区块链类型**
智能合约内容安全	a) 智能合约源代码应符合安全编码规范要求，确保智能合约的安全性；	联盟链和私有链
	b) 应采用技术手段防止对合约内容的篡改；	联盟链和私有链
	c) 智能合约应定义版本号，调用智能合约时应明确记录智能合约版本；	联盟链和私有链
	d) 智能合约应具有向后兼容性，智能合约更新升级或重新部署后，新智能合约能兼容或迁移原智能合约数据；	联盟链和私有链
智能合约运行安全	a) 应提供智能合约的升级和废止功能，智能合约的升级操作应记录在区块中，符合区块链交易要求、遵从交易执行的流程；	联盟链和私有链
	b) 应提供合约安全检测等手段，确保可及时发现和处置出现的问题，降低安全风险；	联盟链和私有链
	c) 应提供方案控制智能合约对外部环境的访问，控	联盟链和私有链

	制隔离执行环境中的智能合约访问其执行环境之外的资源。外部数据的影响范围仅限于智能合约范围内，不应影响区块链系统的整体运行；	
	d) 当智能合约出现错误时，应提供智能合约挂起功能；	联盟链和私有链
	e) 应提供运行载体，如虚拟机等，智能合约应在虚拟机等隔离环境中运行，不能直接运行在参与区块链的节点本地系统上，防止运行智能合约的本地操作系统遭受攻击；	联盟链和私有链
	f) 对于与区块链系统外部数据进行交互的智能合约，外部数据的影响范围仅限于智能合约范围内，不应影响区块链系统的整体运行；	联盟链和私有链
	g) 应对智能合约的操作权限进行限制，避免权限漏洞；	联盟链和私有链
	h) 应严格限制外部合约的调用，防止不受信任的外部合约；	联盟链和私有链
	i) 宜提供有效的方案防止智能合约被恶意滥用，如：多次调用无意义操作，从而造成 DoS 攻击使区块链系统瘫痪。	联盟链
权限控制	a) 接口应根据业务需求做好权限管理，防止未授权的访问和调用，针对不同的用户配置不同的访问权限；	联盟链和私有链
	b) 应设置操作限制，防止攻击者通过大量信息堵塞整个区块链；	联盟链和私有链
	c) 当支持多链架构时，应保证数据的安全隔离；	联盟链和私有链
	d) 应支持区块链节点版本升级，在升级前应在测试环境进行验证，保证升级过程中对业务的平滑过渡；	联盟链和私有链
	e) 区块链节点版本应具有后向兼容性，区块链节点升级后仍支持旧版本的数据；	联盟链和私有链
审计监管	a) 应提供安全审计功能，对重要操作进行审计；	联盟链和私有链
	b) 安全管理机构的所有干预操作行为应被记录实现不可更改并可被查询，做到可审计、可追溯；	联盟链和私有链
	c) 应提供内容监管服务，强化区块链的安全监管；	联盟链和私有链
	d) 应支持安全管理机构接入，在发生特殊突发事件时，可对区块链系统进行干预。	联盟链和私有链

参考文献

[1] CBD-Forum-2017区块链 数据格式规范
[2] CBD-Forum-001-2017区块链 参考架构
[3] CBD-Forum-002-2018区块链 智能合约实施规范
[4] T/SHBTA 002-2019区块链底层平台通用技术要求