国际电信联盟
电信标准化部门

建议书

ITU-T X.1411 (03/2023)

X系列：数据网、开放系统通信和安全性

安全应用和服务（2）– 分布式账簿技术（DLT）安全

区块链即服务（BaaS）安全指南

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
万维网安全（1）	X.1140–X.1149
应用安全（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	X.1350–X.1369
智能交通系统（ITS）安全	X.1370–X.1399
分布式账簿技术（DLT）安全	**X.1400–X.1429**
应用安全（2）	X.1450–X.1459
万维网安全（2）	X.1470–X.1489
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
网络防御	X.1590–X.1599
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
数据保护	X.1770–X.1789
IMT-2020安全	X.1800–X.1819

ITU-T X.1411建议书

区块链即服务（BaaS）安全指南

摘要

ITU-T X.1411建议书为区块链即服务（BaaS）提供了通用的安全指南。首先分析了BaaS的安全威胁和脆弱性，然后提出了BaaS的安全措施。建议书还提出了安全要求，并为建设、运营和使用BaaS的所有活动提供了指南。

区块链即服务（BaaS）已经成为区块链发展的主流，原因是它具有很好的功能，并且得到了业界（特别是来自顶级云提供商）的广泛支持。BaaS为区块链应用提供基础服务和资源，但是它面临着来自区块链核心技术和云平台的安全挑战。因此，就Baas安全性提供指导是非常重要和必要的。

历史沿革

版本	建议书	批准	研究组	唯一识别码*
1.0	ITU-T X.1411	2023-03-03	17	11.1002/1000/15110

关键词

区块链即服务、云计算环境、共识协议、智能合约、安全性

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一识别码，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其他一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其他机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联未收到实施本建议书可能需要的受专利/软件版权保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列ITU-T网站查询适当的ITU-T数据库：http://www.itu.int/ITU-T/ipr/。

目录

ITU-T X.1411建议书

区块链即服务（BaaS）安全指南

1 范围

本建议书规定了区块链即服务（BaaS）的安全指南，并介绍了区块链即服务的定义、结构、安全威胁和漏洞以及措施。构建在BaaS上的BaaS应用的安全性超出了本建议书的范围。

2 参引

下列ITU-T建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献均会得到修订；因此本建议书的使用者应查证是否有可能使用下列建议书和其他参考文献的最新版本。当前有效的ITU-T建议书清单定期出版。本建议书引用某个文件，并非意味着该文件作为单独文件出现时具备建议书的地位。

[ITU-T X.1401] ITU-T X.1401建议书（2019年），*分布式账本技术的安全威胁*。

[ITU-T X.1601] ITU-T X.1601建议书（2015年），*云计算安全框架*。

3 定义

3.1 他处定义的术语

本建议书使用了以下他处定义的术语：

3.1.1 区块链即服务（BaaS）[b-ITU-T Y.3530]：一种云服务类别，向云服务客户提供的能力是使用区块链技术建立区块链平台和开发分散应用的能力。

3.1.2 云服务客户（cloud service customer）[b-ITU-T Y.3500]：以使用云服务为目的的业务关系中的一方。

3.1.3 云服务提供商（cloud service provider）[b-ITU-T Y.3500]：提供云服务的一方。

3.1.4 云服务合作伙伴（cloud service partner）[b-ITU-T Y.3500]：参与支持或辅助云服务提供商或云服务客户或两者活动的一方。

3.1.5 共识（consensus）[b-ITU-T X.1400]：一组交易有效的协议。

3.1.6 点对点（peer-to-peer）[b-ISO 22739]：不依赖中央实体而直接互相分享信息和资源的对等网络的关联方、使用方或其自身。

3.1.7 工作证明（proof of work）[b-ITU-T X.1400]：解决一个困难（昂贵、耗时）问题的共识过程，且产生一个易于他人验证的结果。

3.1.8 智能合约（smart contract）[b-ITU-T X.1400]：在分布式账本系统上编写的程序，它对特定类型的分布式账本系统交易的规则进行编码，编码方式可以通过特定条件进行验证和触发。

3.1.9 威胁（threat）[b-ISO/IEC 27000]：意外事件的潜在原因，可能对系统或组织造成损害。

3.2 本建议书定义的术语

本建议书定义了下列术语：

3.2.1 51%攻击：攻击者通过控制区块的生成，控制足够多的区块链节点或足够多的计算资源来撤销或重写分布式账本系统账本的攻击。

3.2.2 网络分区：一种网络连接场景，其中网络被分成多个不相连的部分。

4 缩写词和首字母缩略语

本建议书使用了下列缩写词和首字母缩略语：

API 应用编程接口

BaaS 区块链即服务

BSC 区块链即服务客户

BSD 区块链即服务开发者

BSP 区块链即服务提供商

BSS 区块链即服务安全开发者

CPU 中央处理器

CSC 云服务客户

CSN 云服务合作伙伴

CSP 云服务提供商

DDoS 分布式拒绝服务

GPU 图形处理器

IAM 身份和访问管理

P2P 点对点

PII 个人身份信息

PoW 工作证明

SDK 软件开发工具包

5 惯例

在本建议书中：

关键词“**须**”（**is required**）指必须严格遵守的要求，如果宣称符合本文件，就不得违反。

关键词“**建议**”（**is recommended**）表示是一项建议的并非需绝对遵守的要求，因此宣称符合本文件时不一定按照该要求行事。

关键词“**可以选择**”（**can optionally**）表示该允许条件属可选项，不带任何建议意味。并非要求供应商的实施方案必须为网络运营商或服务提供商留有该项可以使能的选项或功能，而是指供应商可作为选项提供该功能，并仍宣称符合本规范。

在本建议书的正文及其附录中，有时会出现“**须**”（**shall**）、“**不得**”（**shall not**）、“**应**”（**should**）、“**可**”（**may**）等词语。在这些情况下，这些词语应分别理解为“须”“禁止”“建议”和“可选”。此类短语或关键词出现在附录或明确标记为资料性的材料中时，应解释为没有规范性意图。

6 区块链即服务安全性概述

区块链即服务为区块链开发者和客户提供了一个集成的开发环境，用于创建、开发、测试、托管、部署和操作区块链相关应用。因此，BaaS客户可以利用BaaS平台的核心区块链组件来高效使用和轻松部署区块链网络和应用。

由于区块链基础平台和服务构建于云服务之上，因此有三个主要角色参与BaaS的运行，并与云服务中的角色相对应。

- **区块链即服务提供商（BSP）：**与云计算环境中的云服务提供商（CSP）相对应，BSP由区块链基础设施和平台提供商组成，这些提供商提供区块链即服务。BSP简化了区块链和应用的开发和使用，在所支持的存储、通信、计算和网络支持方面具有基本的区块链相关资源和功能。BSP负责基本区块链资源的安全，并开发提供给BaaS其他角色的工具。
- **区块链即服务开发者（BSD）：**与云计算环境中的云服务合作伙伴（CSN）相对应，BSD负责开发和运行BaaS核心组件，并协助BSP提供区块链服务。BSD还负责已开发的核心组件的安全。
  - **区块链即服务安全开发者（BSS）**是BSD的一种特定类型。BSS作为第三方安全服务提供商，协助BSP增强BaaS的安全性。BSS提供的安全服务包括身份和访问管理（IAM）、审计、入侵检测等。
- **区块链即服务客户（BSC）：**与云计算环境中的云服务客户（CSC）相对应，BSC包括通过BSP直接提供的功能或通过BSD间接提供的应用和服务来请求、访问和使用区块链服务或资源的区块链客户。BSC负责在运行自身的区块链网络和应用时遵守BSP提供的安全规则。亦鼓励BSC与BSP合作监控定制区块链网络的安全，并在必要时报告安全事件。

这些角色之间的交互关系如图1所示。

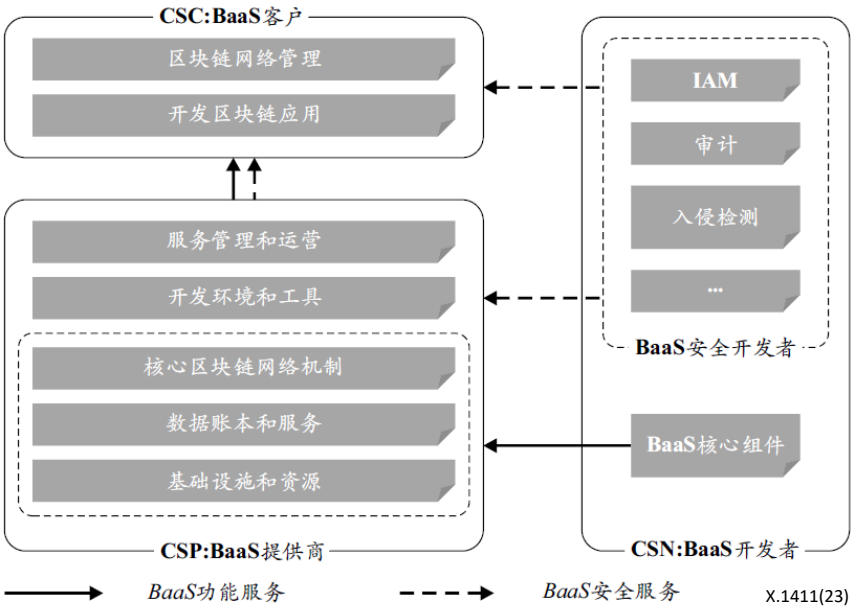

图1 – 区块链即服务中角色的功能和交互

6.1 BSP安全概述

BSP提供区块链核心功能，其中包括智能合约、共识协议、点对点（P2P）连接、加密算法、交易记录、账本管理、节点和资源管理，以及对标准化开发接口和安全服务的支持。BSP的功能和相关的安全挑战如下。

6.1.1 基础设施和资源

BSP提供基础设施，即提供基础的计算、通信和其他资源，以支持区块链网络和应用开发。此类设施可以是物理设备或虚拟设备，如虚拟机和容器。

基础设施面临的挑战包括物理设施的环境风险、后门注入、租户之间的资源共享等。

6.1.2 数据账本和服务

BSP提供链上和链下数据服务，如为BSC存储、管理、查询客户和系统数据。在此方面，链上数据账本保证了防篡改性，而链下数据库支持高效的数据服务。

在数据安全方面，BSP面临以下安全挑战：

– 不可用的数据服务，其中包括网络分区导致的链上和链下数据存储不一致、数据库和存储设施故障导致的数据丢失、数据账本的未授权修改等。

– 隐私泄露，其中包括未经授权访问个人数据、从数据中获取敏感信息、未成功销毁私人数据等。

6.1.3 区块链核心网络机制

BSP在区块链核心网络机制中提供了一组选项，以简化定制区块链网络的设置。区块链核心网络机制由共识协议、P2P连接协议和加密算法组成。BSC可以从所有选项中选择一组特定的网络组件，并设置相应的参数来快速建立定制的区块链网络。

BSP负责应对区块链核心网络机制的安全挑战。此类挑战影响了定制区块链网络的安全性，甚至影响了基于BaaS平台的区块链应用的安全性，原因是BSC直接使用区块链核心网络机制来开发区块链网络和应用。此处所述的安全挑战包括对区块链资源的未授权访问、网络

分区、恶意节点等。例如，由不可用的区块链服务引起的网络分区可能会在分布式区块链网络间达成共识方面造成不可接受的延迟。

6.1.4 开发环境和工具

BSP提供了一个集成的开发环境，提供了应用编程接口（API）、开发工具包和其他开发工具，用于简化区块链应用的开发。由于智能合约是开发区块链应用时的一种本能的区块链机制，BSP还简化了智能合约的部署，并为常见功能（如身份和访问管理）提供了一组智能合约。

相关挑战包括API的不适当的访问控制、不兼容的接口、智能合约的意外运行等。

6.1.5 服务管理和运营

BSP负责根据物理设施、区块链节点、网络连接和所分配的资源以及IAM和其他安全管理功能，监控区块链服务状态并发出告警。BSP还支持和管理BSD提供的区块链相关功能。

相关安全挑战包括不可用的管理功能、不适当的访问管理、未经授权的管理访问、对资源的爆炸性消耗以及BSD提供的区块链相关组件中的风险。

6.2 BSD安全性概述

BSD为BSP开发BaaS核心组件或为所有角色提供安全服务。

6.2.1 开发BaaS核心组件

BSD作为第三方提供商提供BaaS核心组件，如智能合约、加密算法和共识协议。

相关的安全挑战和威胁包括不兼容的接口、不安全的协议设计、协议实施中的后门等。

6.2.2 安全服务

BSS充当BaaS生态系统中所有角色的第三方安全服务提供商。例如，BSS可以为BSP提供入侵检测，为BSD提供代码审计，为BSC提供IAM。

安全挑战包括过时的安全规则、BSS员工的不当操作等。

6.3 BSC安全性概述

BSC使用BSP和BSD提供的服务来构建定制的区块链网络和区块链应用。BSC有两种类型：一种是建立和管理定制区块链网络的管理员，另一种是加入定制区块链网络的成员。对于特定的BSC，它可以是一个定制的区块链网络中的管理员，也可以是另一个定制的区块链网络中的成员。

所有类型的BSC都面临着密钥管理和使用方面的安全挑战。管理员还面临着设置和管理定制区块链网络的安全挑战，如区块链节点、连接和其他资源的不正确设置。

7 对区块链即服务的安全威胁

对BSP、BSD和BSC的威胁可分为三种类型：

– 不安全的技术设计、实施缺陷以及对基本资源、区块链核心功能和区块链服务系统的不当管理。

– BSC、BSD和BSP之间不安全的交互，其中包括不兼容的接口和不安全的供应链。

– 员工的不当操作，其中包括密码的不当使用和存储。

第7.1节至第7.3节列出了每个角色面临的安全威胁。

7.1 对BSP的安全威胁

7.1.1 云服务面临的威胁

由于BSP基于云服务提供基本的区块链资源，因此BSP面临云服务带来的挑战和威胁，如[ITU-T X.1601]第7节和第8节所述。例如，在云服务的共享环境中，对另一个租户的资源分区的未授权访问可能会通过重写或修改其数据账本导致该租户的区块链系统出现区块链分叉。

7.1.2 对区块链核心网络机制的威胁

对共识协议、P2P连接协议和加密引擎的威胁可能是由协议设计中的漏洞、机制实施中的缺陷和不当管理造成的。详情可参考[ITU-T X.1401]第6节。

7.1.3 不可靠的数据服务

分布式数据账本面临的威胁包括区块链资源不足、存储系统缺陷和存储管理不安全，可能导致数据记录不一致、数据丢失、数据篡改和数据泄露。例如，当区块链网络运行时，定制区块链网络的系统和区块链数据会扩展。在BSP没有为定制区块链网络提供足够的存储资源来满足数据扩展的情况下，定制区块链网络会用新数据覆盖旧数据或者直接丢弃新数据，并进而导致定制区块链网络中的数据丢失。另一个例子是，通信或存储设备故障可能导致分布式数据账本中的数据存储不一致。如果故障持续了长时间，所产生的网络分区会导致区块生成、数据查询和其他数据服务的意外延迟。

7.1.4 对开发环境的威胁

BSP提供的集成开发环境、编译环境、智能合约、API、软件开发工具包（SDK）和其他开发辅助功能在此类开发功能的设计、实施、配置和操作过程中面临威胁。例如，API的身份验证缺陷可能导致对基本区块链资源的未授权访问和使用。此外，智能合约在逻辑设计、合约实施和代码管理方面可能存在安全漏洞，如智能合约中的整数溢出和下溢，而这将导致意外的运行结果。

7.1.5 不安全的第三方功能

BSP支持BSD提供的第三方功能，并通过API集成到BaaS平台中。在此方面，第三方功能中的缺陷和恶意软件以及不兼容的API和不适当的API访问控制均可能导致BaaS系统的混乱。

7.1.6 不安全的系统访问

不安全的系统访问包括对区块链设施、数据账本、网络和应用缺乏访问控制或相关的访问控制失当，而这可能导致区块链数据的篡改、对定制区块链网络的入侵以及私人信息的泄露。

7.1.7 内部威胁

BSP员工可能会意外或故意实施恶意行为，例如与未经授权的人员共享密码、将密码放在不安全的地方、泄露个人信息等。内部威胁可能导致私人信息泄露、对定制区块链网络的未经授权访问和区块链服务不可用。

7.1.8 不可靠的供应链

区块链服务平台使用由不同供应商提供的软件和硬件组件。软件和硬件的中断供应将削弱区块链服务的计算、连接和其他资源的能力。在这种情况下，区块链服务的可用性受到威

胁。例如，共识协议工作证明（PoW）依赖于在线区块链节点之间计算能力的竞争，因此计算和连接能力的中断供应会影响基于PoW的区块链网络的共识结果。

此外，软件和硬件以及开源区块链架构中的恶意软件和可利用的漏洞可能导致不可预料的区块生成、拒绝服务、数据泄漏和误用等。

7.1.9 对物理环境的威胁

火灾、洪水、雷电和针对基础设施的其他环境灾难可能导致物理设施无法提供通信、计算和其他基础资源。例如，故意或意外断电可能导致区块链节点的一个分区离线。在这种情况下，共识过程由较少数量的区块链节点控制，将导致不正确的共识结果和区块生成中的额外延迟。

7.2 对BSD的安全威胁

7.2.1 对第三方功能的威胁

BSD作为第三方提供商提供区块链核心组件、区块链安全机制和区块链应用开发功能。相关威胁包括区块链核心组件固有的安全漏洞、此类第三方功能的实施缺陷、接口不兼容以及接口的访问控制不安全。

除此之外，BSD员工的恶意行为还可能导致私人信息泄露、第三方功能中的后门以及安全功能的意外操作。

7.3 对BSC的安全威胁

7.3.1 密钥泄漏和丢失

BSC自行或通过第三方服务管理密钥。密钥存储不当、密钥文件损坏或不可靠的第三方密钥服务均可能导致密钥丢失或泄露，从而导致BSC资产丢失、隐私泄露和定制区块链网络的紊乱。

7.3.2 定制区块链网络管理不当

BSC基于BSP和BSD提供的区块链功能建立自身的定制区块链网络并部署安全机制。在此方面，定制区块链网络和安全机制的不当配置将对定制区块链网络造成威胁。例如，如果BSC为定制区块链网络的运行分配的存储资源不足，那么定制区块链网络可能无法更新区块链数据，最终导致区块链数据账本不一致。

8 区块链即服务的安全要求

8.1 定制区块链网络的安全配置

建议BSP就定制区块链网络的配置提供建议，以满足BSC的安全要求。此外，建议BSP就在定制区块链网络上部署必要的安全机制提供建议。

a) BSP须规定节点总数的建议范围。

b) BSP须规定在线节点的最小数量，以避免区块链网络的51%威胁和其他已知威胁。

c) BSP须规定每个节点的邻居的最小数量，以避免区块链网络分区。

d) 建议BSP规定所建议的节点类型，并规定每种类型的数量和权限。

e) 建议BSP规定每种类型节点的最小存储资源、中央处理器（CPU）和图像处理单元（GPU）。

f) 建议BSP根据节点配置规定所建议的共识协议和点对点协议。

g) 建议BSP为定制区块链网络提供基本的安全功能，其中包括IAM和密钥管理。

h) BSP可以选择提供定制区块链网络配置的安全评估。BSP须向BSC提供相关的安全建议和解决方案。

8.2 身份和访问管理

建议BSP为BaaS系统和定制区块链网络提供身份和访问管理功能。部署身份和访问管理功能不仅是为了保护身份，也是为了方便访问管理、身份验证和授权。

a) BSP须为BaaS系统提供身份注册和注销功能。

b) 建议BSP为定制区块链网络提供身份注册和注销功能。

c) BSP须为BaaS系统提供帐户访问管理，以区分BSP、BSC和BSD。

d) 建议BSP在定制区块链网络中提供帐户访问管理。任何定制区块链网络均应有一个或多个具有不同访问权限的客户角色。

e) BSP须为BaaS系统提供访问认证。每个身份只能根据其访问权限访问资源。

f) 建议BSP为定制区块链网络提供访问认证。

g) BSP可以选择提供细致访问管理功能，比如基于角色的访问控制功能。

h) BSP可以选择监控访问IP、访问账户、访问设备等的访问活动频率。访问活动包括注册、注销、密钥更新等。

8.3 密钥管理

建议BSP提供密钥管理功能，以保护密钥生成、存储、分发、使用、备份、恢复和撤销的安全性。

a) BSP须提供全面的密钥管理方案，明确密钥信息和管理流程。

b) BSP须评估用于生成密钥的随机数算法和其他参数的安全性。随机数算法须满足随机性和不可预测性。

c) 建议BSP支持第三方密钥管理功能。在提供给BSC之前，须对第三方密钥管理功能的安全性进行评估和保证。

d) 建议BSP为注销和可疑账户提供密钥撤销功能。

e) 建议BSP为丢失的密钥提供密钥检索功能。只有经过身份验证的帐户才能访问密钥检索功能。

f) 建议BSP要求BSC定期更新密钥。更新周期须根据安全级别而有所不同。

g) 建议BSC在定制区块链网络中部署密钥管理功能。

h) 根据定制区块链网络中部署的密钥管理功能，BSC须掌握并遵循密钥使用、存储、检索和撤销的安全程序。

i) 建议BSC按照密钥管理功能中的预定义向BSP报告可疑的密钥使用情况。

j) BSP可以选择对主密钥和秘密密钥使用双方或多方密钥存储方案。

8.4 隐私保护

建议BSP为个人身份信息（PII）的收集、访问和其他操作提供保护。

a) BSP须遵守与隐私保护相关的国家和地方法规、政策和立法，如PII收集和PII存储。

b) BSP须对所展示的PII进行去身份化。

c) BSP须部署安全措施，以保证在BSC要求时，链上的PII可以被完全删除，例如使用基于变色龙哈希算法的区块链技术，或者在链外存储PII。

d) 建议BSP邀请专业机构对有关PII的敏感操作进行审计。

8.5 加密引擎安全性

建议BSP保证部署在定制区块链网络中的加密引擎的安全性。

a) BSP须支持主流加密算法，且其安全性已经过公开验证。

b) BSP须邀请专业机构对加密引擎的安全性进行审计。

c) 建议BSP支持BSD提供的加密引擎。建议BSD提供加密引擎的安全评估结果。

8.6 点对点连接的安全性

建议BSP保证点对点连接能够抵御不可靠和恶意的节点。

a) BSP须提供认证方案来管理对点对点网络的访问。

b) BSP须使用密码技术在分布式节点之间建立安全的传输通道。

c) BSP须支持具有可靠性和可扩展性的点对点协议。可靠性指的是断开的节点在重新连接后与其他节点保持一致。可扩展性指的是在区块链网络正常运行的情况下，协议支持动态或静态添加或删除节点。

d) BSP须支持任何节点均有多个邻居的点对点协议。

e) 建议BSP支持点对点协议，以确保任何断开的节点均不会导致网络分区。

f) 建议BSP提供点对点网络的实时拓扑。

g) 如果点对点网络面临分区或恶意节点，建议BSP提供告警。

8.7 共识机制的安全性

建议BSP保证共识机制的设计和操作是安全的。

a) BSP须在安全性已被公开证明或评估的情况下提供共识算法。

b) BSP须支持BSC部署BSD提供的共识算法。

c) BSP须向BSC提供共识算法的安全评估。安全评估应包括共识节点的阈值数量、所建议的共识频率等。

d) BSP须保证共识节点在加入共识之前被认证。

e) BSP须监控共识过程，并评估共识周期、共识节点和共识结果。

f) 当监控的共识过程被评估为异常时，建议BSP提供告警和解决方案。

8.8 智能合约的安全性

建议BSP为智能合约提供全面的生命周期管理，其中包括智能合约的创建、部署、升级、触发、执行和废除。

a) BSP须提供智能合约的代码规范、逻辑要求和其他规范性指导。

b) 建议BSP为运行智能合约提供一个可信的隔离环境，如沙箱。

c) BSP须为智能合约提供适当的访问管理，以限制恶意操作或防止错误的智能合约感染其他合约。

d) BSP须支持智能合约的安全应急响应机制。

e) BSP须在资源消耗和执行时间方面限制智能合约的复杂性。

f) 建议BSP通过智能合约监控区块链资源的过度消耗。

g) 当智能合约超出资源限制时，建议BSP支持智能合约的终止。

h) 建议BSP提供技术解决方案，以防止与智能合约相关的分布式拒绝服务（DDoS）攻击。

i) 建议BSP让BSD提供自动检测智能合约源代码和智能合约字节码安全漏洞的功能。

j) 建议BSP让BSD监控智能合约活动，以便发现智能合约的早期预警异常行为。

8.9 资源监控

建议BSP监控BaaS中的资源消耗情况，并在资源状态异常时发出告警。

a) 建议BSC允许BSP监控定制区块链网络中节点的资源消耗，其中包括存储、计算、CPU、网络连接、在线状态、在线持续时间等。

b) 当定制区块链网络的节点面临资源短缺时，建议BSP向BSC提供资源短缺告警。BSP须向BSC提供解决方案，以缓解资源短缺。

c) 建议BSC允许BSP监控定制区块链网络在区块生成速率、区块生成器、区块大小等方面的网络状态。

d) 当监控到网络状态异常时，建议BSP向BSC提供入侵警报。BSP须向BSC提供相应的异常分析、相关的异常节点信息和所建议的解决方案。

8.10 入侵检测系统

建议BSP提供并更新防止恶意代码和其他入侵的机制。

a) BSP须提供智能合约安全规则和漏洞库。BSP须为漏洞检测提供通用形式的访问接口。

b) BSP须安装反恶意软件或配置具有相应功能的软件，以检测和清除恶意软件。

c) 建议BSP在每个区块链节点中提供恶意代码防护，并在访问区块链网络之前消除恶意代码。

d) 建议BSP对恶意代码防范机制做出规定，其中包括定期升级恶意代码库以及定期查杀恶意代码。

e) 建议BSP让BSD定期评估针对恶意代码攻击的技术措施的有效性。

8.11 安全审计

建议BSP有一个或多个BSD对区块链基础设施、源代码和其他基本功能进行安全审计。

a) 建议BSP在区块链服务上线前，选择多个BSD对区块链基础软件、网络等运行环境进行安全评估和审计，以确保基础设施层面的安全风险可控。

b) 建议BSP至少有一个BSD对源代码进行安全审计，且主要针对源代码层面的风险和质量问题。

c) 建议BSD向BSP提供源代码审计报告，报告中应列出源代码的合规/违规项目和修订建议。

d) 建议BSP让BSD对IAM功能进行评估，以确保不存在私钥泄露、用户信息泄露等风险。

8.12 第三方功能管理

建议BSP保证第三方功能按照预定义的方式安全运行。

a) BSP须阐明第三方提供商的安全和功能要求。

b) BSP须与第三方服务提供商签订服务组件合作协议，明确双方的义务和责任。

c) 建议BSP监控或审计第三方服务，并根据签署的协议评估其服务。

8.13 供应链安全

建议BSP保证其供应链能够抵御恶意供应商和供应商变更。

a) BSP须制定供应链安全管理策略和程序，其中包括供应链参与者的安全管理标准。

b) BSP须定期评估其基础设施中的供应链漏洞以及系统中的开源使用情况。

c) 建议BSP将区块链即服务系统中的供应链风险告知BSC。

d) BSP须确认其不可或缺的软件和硬件供应商的多样性。

表1 – BaaS的安全要求

安全威胁		安全要求												
		安全配置	IAM	密钥管理	隐私保护	加密引擎安全性	P2P连接安全性	共识机制安全性	智能合约安全性	资源监控	入侵检测系统	安全审计	第三方功能管理	供应链安全
BSP	7.1.1	✓	✓	✓	✓				✓			✓	✓	✓
	7.1.2					✓	✓	✓	✓		✓	✓	✓	✓
	7.1.3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	7.1.4							✓	✓	✓	✓			
	7.1.5										✓	✓	✓	✓
	7.1.6		✓	✓										
	7.1.7		✓										✓	
	7.1.8											✓	✓	✓
	7.1.9												✓	
BSD	7.2.1			✓	✓	✓	✓	✓		✓	✓		✓	
BSC	7.3.1		✓	✓										
	7.3.2	✓								✓			✓	

参考文献

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T Y.3500] Recommendation ITU-T Y.3500 (2014) | ISO/IEC 17788:2014, *Information technology – Cloud computing – Overview and vocabulary*.

[b-ITU-T Y.3530] Recommendation ITU-T Y.3530 (2020), *Cloud computing – Functional requirements for blockchain as a service*.

[b-ISO 22739] ISO 22739:2020, *Blockchain and distributed ledger technologies – Vocabulary*.
<https://www.iso.org/standard/73771.html>

[b-ISO/IEC 27000] ISO/IEC 27000:2018(en), *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.
<https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

ITU-T 建议书系列

系列 A	ITU-T 工作的组织
系列 D	资费及结算原则和国际电信/ICT 的经济和政策问题
系列 E	综合网络运行、电话业务、业务运行和人为因素
系列 F	非话电信业务
系列 G	传输系统和媒介、数字系统和网络
系列 H	视听及多媒体系统
系列 I	综合业务数字网
系列 J	有线网络和电视、声音节目及其他多媒体信号的传输
系列 K	干扰的防护
系列 L	环境与 ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列 M	电信管理，包括 TMN 和网络维护
系列 N	维护：国际声音节目和电视传输电路
系列 O	测量设备的技术规范
系列 P	电话传输质量、电话设施及本地线路网络
系列 Q	交换和信令，以及相关联的测量和测试
系列 R	电报传输
系列 S	电报业务终端设备
系列 T	远程信息处理业务的终端设备
系列 U	电报交换
系列 V	电话网上的数据通信
系列 X	**数据网、开放系统通信和安全性**
系列 Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列 Z	用于电信系统的语言和一般软件问题

瑞士印刷
2023年，日内瓦