



T/CECS G XXXX: 2023

中国工程建设标准化协会标准

Standard of China Association for Engineering Construction  
Standardization

收费公路联网收费区块链数据  
交换标准

Technical Standards for Toll Road Blockchain Data Exchange

中国工程建设标准化协会 发布

Issued by China Association for Engineering Construction Standardization

征求意见稿

中国工程建设标准化协会标准

# 收费公路联网收费区块链数据交换标准

Technical Standards for Toll Road Blockchain Data Exchange

T/CECS G: xxxx-2023

主编单位：交通运输部路网监测与应急处置中心

批准部门：中国工程建设标准化协会

实施日期：2023年XX月XX日

人民交通出版社股份有限公司

北京

# 前 言

根据中国工程建设标准化协会公路分会《关于开展 2022 年第一批中国工程建设标准化协会标准(CECS G)制修订项目编制工作的通知》(中建标公路[2022]91 号)的要求,由交通运输部路网监测与应急处置中心承担《收费公路联网收费区块链数据交换标准》的制订工作。

编写组在总结 ETC 收费十余年来工程经验和相关科研成果的基础上,为规范收费公路联网收费区块链技术的主要技术要求,指导收费公路联网收费区块链系统建设,完成了本标准的编写工作。

本标准分为 8 章,主要包括:1 总则、2 术语与符号、3 基本规定、4 总体框架、5 通用基础要求、6 同链调用、7 跨链访问、8 链外协同。

请注意本标准的某些内容可能直接或间接涉及专利,本标准的发布机构不承担识别这些专利的责任。

本标准基于通用的工程建设理论及原则编制,适用于本标准提出的应用条件。对于某些特定专项应用条件,使用本标准相关条文时,应对适用性及有效性进行验证。

本标准由中国工程建设标准化协会公路分会负责归口管理,由交通运输部路网监测与应急处置中心负责具体技术内容的解释,在执行过程中如有意见或建议,请函告本标准日常管理组,中国工程建设标准化协会公路分会(地址:北京市海淀区西土城路 8 号;邮编:100088;电话:010-62079839;传真:010-62079983;电子邮箱:shc@rioh.cn),或孙树垚(地址:北京市朝阳区安定路 5 号院 10 号楼外运大厦 A 座;邮编:100029;电子邮箱:ssy92729@163.com),以便修订时研用。

**主 编 单 位:** 交通运输部路网监测与应急处置中心

**参 编 单 位:** 北京航空航天大学

北京网路智联科技有限公司

北京微芯区块链与边缘计算研究院

辽宁省高速公路运营管理有限责任公司

辽宁高速通智慧出行有限责任公司

**主 编:** 刘 旭

**主要编制人员:** 刘 旭 宋 杰 谷 岩 孙树垚 李 俐 韩 旭  
李 勇 赵 亮 任 政 周 游 王道煜 王海泉  
杜博文 赵洁洁 马瀚元 李宇轩 蔡 雨 何辰之  
谢 悦 张 祎 娄文超 罗雅倪 唐 琳 黄 瑾  
展恩宁 张友权 葛大明 朱瑞新 段 拙

**主 审:** 孙兴焕

**参与审查人员:**

**参 加 人 员:**

征求意见稿

## 目 次

1	总则.....	1
2	术语和符号.....	1
	2.1 术语定义.....	1
	2.2 符号.....	8
3	基本规定.....	8
	3.1 共性特征.....	8
4	技术要求.....	错误!未定义书签。
	4.1 基本要求.....	错误!未定义书签。
	4.2 服务支持和应用支持方面的技术要求.....	错误!未定义书签。
	4.3 安全方面的技术要求.....	错误!未定义书签。
5	收费公路联网收费区块链框架和能力.....	错误!未定义书签。
	5.1 系统架构.....	错误!未定义书签。
	5.2 数据流向.....	错误!未定义书签。
	5.3 基础层.....	错误!未定义书签。
	5.4 核心层.....	错误!未定义书签。
	5.5 服务层.....	错误!未定义书签。
	5.6 应用层.....	错误!未定义书签。
6	收费公路联网收费区块链系统的主要流程.....	错误!未定义书签。
	6.1 存证数据上链.....	错误!未定义书签。
	6.2 存证信息取证.....	错误!未定义书签。
7	数据要求.....	错误!未定义书签。
	7.1 上链数据.....	错误!未定义书签。
	7.2 访问权限.....	错误!未定义书签。

# 1 总则

1.0.1 本标准规范指导收费公路联网收费链上数据在同构区块链间交换、异构区块链间交换、链与非链系统间交换、协同方式，支撑交易对账、争议处理等业务场景所需的跨省数据交换功能，从总体框架、通用基础要求、同链调用、跨链访问、链外协同等方面内容，制定本数据交换标准。

1.0.2 区块链收费公路联网收费数据系统建设除应符合本标准规定外，尚应符合国家现行有关标准的规定。

# 2 术语和符号

## 2.1 术语定义

GB/T 25069—2010《信息安全技术术语》、JR/T0184—2020《金融分布式账本技术安全规范》、GB/T 18277—2000《公路收费制式》、DB14/T 1253—2016《高速公路电子不停车收费(ETC)服务网点建设和管理规范》、DB11/T 1165.5—2019《收费公路联网收费系统第5部分：清分结算规则》、JTGB10-01-2014《公路电子不停车收费联网运营和服务规范》及CBD-Forum-001—2017《区块链参考架构》中界定的以及下列术语和定义适用于本文件。

### 2.1.1

#### **区块链 blockchain**

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可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。注：事务处理包括但不限于可信数据的产生、存取和使用等。

[CBD-Forum-001—2017，定义 2.2.1]

### 2.1.2

#### **区块链技术 blockchain technology**

一种由多方共同维护，使用密码学保证传输和访问安全，能够实现数据一致存储、防篡改、防抵赖的技术体系。

### 2.1.3

#### **区块链产品 blockchain product**

实现了区块链技术的软件产品。

### 2.1.4

#### **区块链节点 blockchain node**

安装了区块链产品，维护区块链数据的设备。

### 2.1.5

#### **区块链系统 blockchain system**

由多个区块链节点组成的分布式系统。

### 2.1.6

#### **共识 consensus**

区块链系统中各节点间达成一致制定的过程。

### 2.1.7

#### **共识算法 consensus algorithm**

区块链系统中各分布的节点对事务或状态的验证、记录、修改等行为达成一致确认的方法。

[CBD-Forum-001—2017，定义 2.2.3]

### 2.1.8

#### **共识协议 consensus protocol**

分布式帐本系统中各节点间为达成一致采用的计算方法。

[JR/T0184—2020, 定义 3.17]

### 2.1.9

#### **数据完整性 data integrity**

数据没有遭受以未经授权方式所作的更改或破坏的特性。

[GB/T 25069—2010, 定义 2.1.36]

### 2.1.10

#### **保密性 confidentiality**

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069—2010, 定义 2.1.1]

### 2.1.11

#### **一致性 consistency**

在某一系统或构件中，各文档或各部分之间统一的、标准化的和无矛盾的程度。

[GB/T 25069—2010, 定义 2.1.62]

### 2.1.12

#### **摘要算法 digest algorithm**

又称摘要函数（或称 Hash 函数），通常通过将任意长度的消息输入变成固定长度的短消息输出来保障数据的完整性。

[CBD-Forum-001—2017, 定义 2.2.4]

### 2.1.13

#### **智能合约 smart contracts**

以数字形式定义的能够自动执行条款的合约。注：在区块链技术领域，智能合约是指基于预定事件触发、不可篡改、自动执行的计算机程序。

[CBD-Forum-001—2017, 定义 2.2.7]

#### 2.1.14

##### **公有链 public blockchain**

任意节点均可接入,所有接入节点均可参与共识和读写数据的一类区块链部署模型。

#### 2.1.15

##### **联盟链 consortium blockchain**

由一组利益相关的参与者使用,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一类区块链部署模型。

#### 2.1.16

##### **私有链 private blockchain**

仅由单个实体使用,仅有授权的该使用方节点可接入,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。

#### 2.1.17

##### **同链调用 same chain call**

在同一个区块链系统上的多个智能合约之间的相互调用。

#### 2.1.18

##### **跨链访问 cross chain access**

数据从一个区块链系统传递到另一个区块链系统的过程。

#### 2.1.19

##### **链外协同 out-of-chain collaboration**

非区块链系统与区块链系统的相互交互,包含区块链系统访问非区块链系统

获取数据，及非区块链系统对区块链系统的访问。

#### 2. 1. 20

##### **加密 encipherment/encryption**

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

[GB/T 25069—2010，定义 2.2.2.60]

#### 2. 1. 21

##### **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受者用以确认数据单元的来源和完整性，并保护数据防止被伪造或抵赖。

[GB/T 25069—2010，定义 2.2.2.176]

#### 2. 1. 22

##### **散列/杂凑函数 hash function**

将比特串映射为固定长度的比特串的函数，该函数满足下列两特性：  
——对于给定输出，找出映射为该输出的输入，在计算上是不可行的；  
——对于给定输入，找出映射为同一输出的第二个输入，在计算上是不可行的。

注：计算上的可行性取决于特定安全要求和环境。

[GB/T 25069—2010，定义 2.2.2.166]

#### 2. 1. 23

##### **访问控制 access control**

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

[GB/T 25069—2010, 定义 2.2.1.42]

#### 2. 1. 24

##### **收费公路 toll highway**

根据国家法规向公路使用者收取通行费的公路。

[GB/T 18277—2000, 定义 3.1]

#### 2. 1. 25

##### **收费站 toll station**

收费站是收费业务的基层管理单位，配备有相应的收费设施。

[GB/T 18277—2000, 定义 3.9]

#### 2. 1. 26

##### **电子不停车收费 electronic toll collection**

在不停车的条件下，应用无线电射频识别及计算机等技术自动完成对通过车辆的识别，收费操作、车道设备控制和收费数据处理的收费方式。

[DB14/T 1253—2016, 定义 3.1]

#### 2. 1. 27

##### **清分 clearing**

统计各参与方应收/付款金额并与相关参与方核对数据操作的过程。

[DB11/T 1165.5—2019, 定义 3.2]

#### 2. 1. 28

##### **结算 settlement**

ETC 运营中心与各代理机构进行数据对账、争议处理及划账的过程。

[DB14/T 1253—2016, 定义 3.18]

2. 1. 29

**争议交易 dispute transaction**

参与方对收费账务结算结果提出异议的原始交易。

[JTG B10-01-2014, 定义 2.0.6]

征求意见稿

## 2.2 符号

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

2.2.2 CA: 证书授权 (Certificate Authority)

2.2.3 ETC: 电子收费系统 (Electronic Toll Collection System)

2.2.4 ID: 标识 (Identity)

2.2.5 IP: 互联网协议地址 (Internet Protocol Address)

2.2.6 OBU: 车载单元 (On board Unit)

2.2.7 PKI: 公钥基础设施 (Public Key Infrastructure)

2.2.8 RSU: 路侧单元 (Roadside Unit)

2.2.9 SDK: 软件开发工具包 (Software Development Kit)

2.2.10 SM: 国家商用密码算法 (ShangMi)

2.2.11 TAC: 交易认证码 (Transaction Authorization Cryporgram)

## 3 基本规定

### 3.1 共性特征

3.1.1 收费公路联网收费区块链数据交换系统应符合功能统一、数据标准、融合共享、安全可靠的基本原则。

3.1.2 收费公路联网收费区块链数据交换系统应支持数据上链,存证信息取证与核验等基本能力。

- 3.1.3 收费公路联网收费区块链数据交换系统应包含众多参与方,包含省中心以及省内联网收费站。
- 3.1.4 收费公路联网收费区块链数据交换系统应当具备完整的记账、交易性能,支持一定程度的高并发请求。
- 3.1.5 收费公路联网收费区块链数据交换系统应充分考虑用户操作习惯,将区块链技术作为底层支持技术,并通过开发各类接口与上层业务平台或与操作界面相连接。
- 3.1.6 收费公路联网收费区块链数据交换系统应保证系统达到信息系统安全等级二级,区块链系统应满足各类国密算法及共识机制,并建立严格的节点准入规则,保障系统安全。
- 3.1.7 收费公路联网收费区块链数据交换系统应支持拓展应用场景。在统一标准、统一业务运营规则、统一客户服务规范的基础上,构建以联机交易为主、风险可控的准联机交易为补充的业务体系。
- 3.1.8 基于区块链技术的收费公路联网收费区块链数据交换系统应与银行等金融机构互通,确保其承担可控的资金垫付和兜底风险,同时提高 ETC 车辆的停车费支付成功率。

## 4 总体框架

### 4.1 数据交换体系

基于公路联网收费总体要求,初步构建数据交换体系如图 4.1 所示。

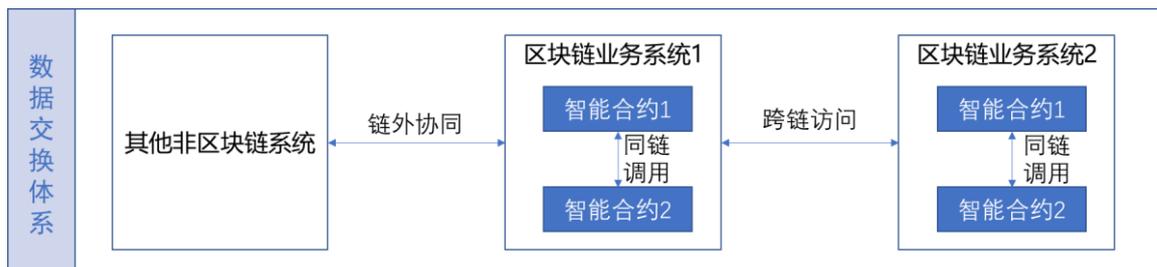


图 4.1 公路联网收费区块链数据交换体系

数据交换体系主要由区块链业务系统和非区块链系统两部分构成。区块链业务系统内部包含多个智能合约，智能合约之间可进行同链调用；而在多个区块链业务系统之间则使用跨链工具进行互相访问。同时，区块链业务系统与非区块链业务系统之间构成链外协同的关系。

## 4.2 数据交换总体框架



图 4.2 公路联网收费区块链数据交换体系

在数据交换体系的基础上，初步构建数据交换总体框架，包括：链外协同、跨链访问、同链调用及其他基础要求。

### 4.2.1 链外协同

链外协同包括区块链对外提供服务和区块链访问非区块链系统两部分。对区块链的对外调用接口服务、访问控制、联机访问提出要求。

### 4.2.2 跨链访问

跨链访问包括同构区块链和异构区块链两种情况。对区块链的跨链查询、跨链写入及权限进行要求。

### 4.2.3 同链调用

同链调用包括同合约交互及不同合约交互两种情况。对区块链多合约支持、数据隔离、访问支持、访问控制、协同原则里提出要求。

#### 4.2.4 基础要求

基础要求包括数据格式要求及研发支持要求两种情况。对区块链数据格式及研发支持提出要求。

## 5 通用基础要求

### 5.1 数据格式要求

#### 5.1.1 区块数据格式要求

收费数据基础数据元编码对象所包含数据类型应分为基础数据类型与扩展数据类型，基础数据类型应包括布尔型、无符号整型、有符号整型、浮点数、字符串，其中整型数字的长度应满足 1 字节到 128 字节，浮点数的长度应包括 32 字节、64 字节；复杂数据类型应包括列表、字典、结构体。

#### 5.1.2 收费数据格式要求

收费数据元编码对象应包含以下字段：计费交易编号（包括收费门架编号、交易批次号、主备卡标记、流水号）、交易金额、通行介质类型、OBU 单/双片标识、OBU 编号、ETC 卡编号、CPC 卡编号、PSAM 卡脱机交易序列号、实际收费车辆车牌号码+颜色、识别的车牌号码+颜色、计费车型、识别的车型、车种、TAC 码、交易类型标识、终端机编号、收费单元编号、收费单元名称、交易的服务类型、算法标识、优惠金额、计费模块和计费参数版本号、车辆识别流水号、入口车道编号、通行 ID。

#### 5.1.3 通行数据格式要求

通行数据元编码对象应包含以下字段：交易编号（包括车道编号、交易批次号、流水号）、出入类型、通行介质类型、介质编码、OBU 单/双片标识、实际车辆车牌号码+颜色、识别的车牌号码+颜色、收费车型、车种、入口收费站名称、出口收费站名称、重量、轴数、特情类型、车牌识别流水号、入口车道编号、入

口车道 hex、通行 ID、收费站车牌识别图片、门架车牌识别图片。

### 5.1.4 监测数据格式要求

监测数据元对象分为收费车道监测数据元和收费门架监测数据元。其中收费车道监测数据元应包含以下字段：收费车道监测流水号（包括车道编号、监测数据生成时间）、收费站编号、车道类型、入/出口车道标识、当前稽查灰名单版本号、当前稽查黑名单版本号、当前 OBU 状态名单版本号、用户卡黑名单版本号、CPC 卡灰名单版本号、车道状态、RSU 状态、车道控制器、对应站级服务器、读卡器状态、自动栏杆机、移动支付设备、车牌识别状态、车间起状态、轴型检测器状态、光栅状态、车道摄像机状态、费额显示屏状态、信息提示屏状态、通行信号灯状态、ETC 情报板状态、入口治超设施状态、操作系统版本号、车道软件版本号。收费门架监测数据元应包含以下字段：ETC 门架监测流水号（门架后台编码）、计费模块和计费参数版本号、RSU 状态、车牌识别状态、车检器状态、车型检测器状态、载重检测器状态、操作系统版本号、车道软件版本号。

## 5.2 研发支持要求

在收费数据基础数据元编码中，每一收费数据基础数据元编码对象仅有一个赋予它的代码，一个代码只唯一表示一个收费数据基础数据元编码对象。

## 6 同链调用

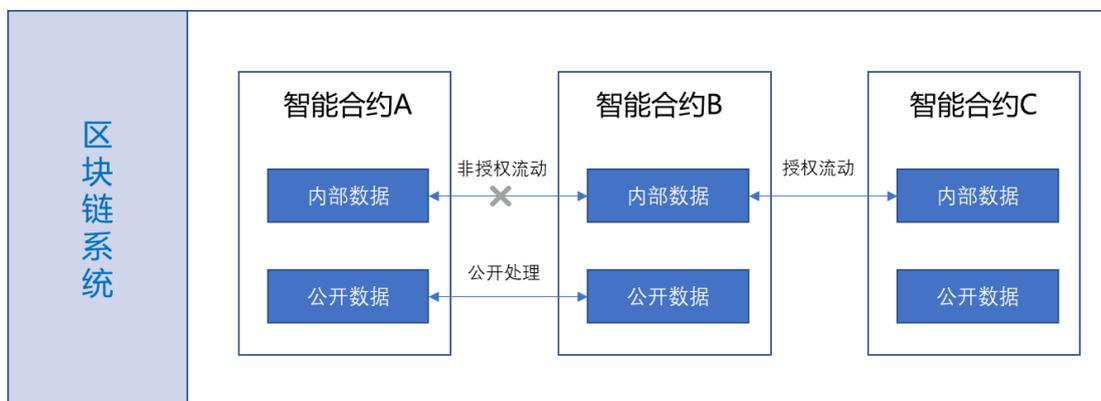


图 6.1 区块链同链调用

## 6.1 多合约支持要求

## 6.2 合约间查询要求

合约间查询是指合约之间进行链上调用的过程。合约间互相调用时，宜使用“检查-生效-交互”模式。合约间查询应实现：

- (1) 访问已部署的合约库，并获取数据。
- (2) 利用已部署的合约进行多功能组合，如查询监测数据时同时获取收费数据。

### 6.2.1 合约间写入要求

合约间写入是指调用已有合约进行数据写入的过程。合约间写入时，应实现：

- (1) 访问已部署的合约库，并写入数据。
- (2) 对已部署的合约进行合约复用，实现数据写入权限的保护。

## 6.3 数据隔离要求

系统应根据信息的重要程度和不同类别，采取不同的保护措施，实施分类防护。并根据系统和数据的重要程度和敏感程度不同，进行分域存储，建议系统满足：

- (1) 按照业务系统信息和应用分类的安全需求，划分为内部数据处理区域和公开数据处理区域。
- (2) 要求对不同区域实施安全隔离，应能够实施各安全域间的信息流控制，防止域间信息的非授权流动。

### 6.3.1 隐私数据要求

所有隐私数据应在内部数据处理区域中，仅通过部分合约向外提供访问渠道。建议系统满足：

- (1) 所有涉及隐私数据的合约调用需系统权限，仅向部中心等参与者开放。
- (2) 对隐私数据使用摘要上链形式，避免用户隐私直接泄露。

## 6.4 访问控制

按照公路联网收费系统的功能及其安全要求，宜明确各安全域的用户访问控制策略，以限定不同类型用户的接入访问区域，防止非授权访问。

### 6.4.1 控制权限要求

不同用户的控制权限要求如下：

- (1) 互联网用户可接入访问公开数据处理区域。
- (2) 仅允许授权用户接入访问安全管理区域。
- (3) 宜禁止接入用户的越权访问、跨区域访问，防止内部数据的泄露与破坏。

## 6.5 协同原则

在区块链上部署的多个智能合约间，应具备协同原则，利用可靠的权限管理和授权机制来保障区块链资源的信息安全。协同原则宜：

- (1) 将合约间的权限控制细化到分区以及资源的具体接口。
- (2) 对新接入的节点实时同步和执行来自权限管理合约的权限策略。
- (3) 控制和记录合约间的操作，实时保障跨链业务的信息安全。

## 7 跨链访问

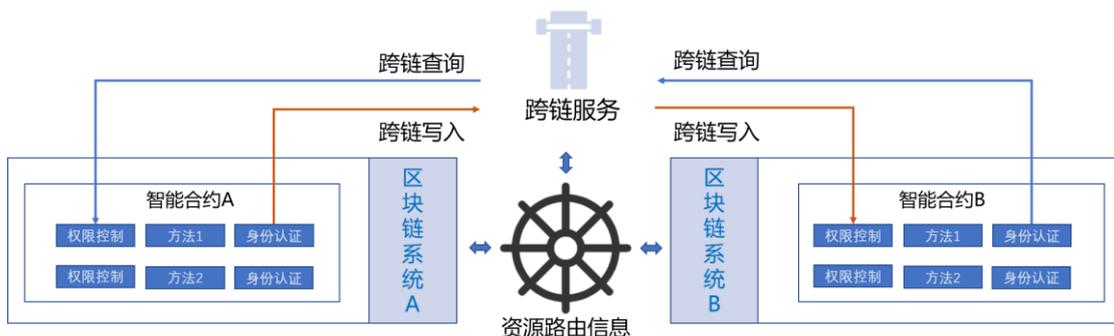


图 7.1 区块链跨链访问

## 7.1 跨链功能要求

区块链应用业务场景应支持链间的互通，一些链的应用系统的业务结果可以触发另一些分布式系统的业务运行，以此构建公路联网收费系统的区块链业务应用协作平台。跨链功能应能使系统连通更多业务场景，进一步挖掘区块链系统的应用价值。

系统应能处理不同省区块链平台间以及平台内不同底层架构的区块链应用交互问题，为公路联网收费平台业务的运行提供保障。

### 7.1.1 数据隔离要求

为了确保数据交换的透明度和可追溯性，系统应在适当的程度上隔离各省的区块链系统数据，即各省主要访问自省的区块链系统及其中的数据。在省际区块链系统的数据安全防护方面，系统应采取有效的措施，如在网络层面适度实现物理隔离，以限制各省直接访问其他省的区块链系统。从而保障数据安全隔离，保证数据生产、存储、传输、访问、使用全流程的安全。

### 7.1.2 跨链查询要求

定制交换数据安全性要求应包括以下几个方面：

- (1) 定制交换数据源可信。应支持基于密码技术的对数据源生成者的身份认证，确保交换数据源的真实性和不可否认性。
- (2) 定制交换数据完整。应支持对交换信息的完整性验证，防止交换过程中的木马夹带攻击与信息非法篡改。
- (3) 定制交换数据保密。应支持对交换信息的加密存储和传输，确保交换信息的保密性。
- (4) 定制交换数据过滤。应支持基于域间信息安全交换策略的信息过滤；应支持不同粒度的信息过滤；应支持基于黑/白名单的过滤规则的过滤管理。

### 7.1.3 跨链写入要求

在域间进行信息写入时，需要保证交换数据的安全性。包括：

- (1) 交换数据的安全性主要包括交换数据源可信、交换信息保密、交换信息完整及交换内容过滤等。
- (2) 交换数据源可信应支持交换数据生成者对交换数据的数字签名, 确保交换数据源的真实性和不可否认性。
- (3) 交换信息保密宜支持对交换信息的加密存储和传输, 确保交换信息的保密性。
- (4) 交换信息完整宜支持对交换信息的完整性验证, 防止交换过程中的木马夹带攻击与信息非法篡改。
- (5) 交换内容过滤应支持对交换信息实施基于安全交换策略的内容过滤。

## 7.2 跨链访问控制要求

跨链互操作过程中，系统需要跨链管道的约束信息为基础进行交互，并将该信息应用于跨链交互中的权限判断，安全验证等操作中。管道约束信息宜包括：

- (1) 权限信息（跨链双方账户信息）
- (2) 业务路由信息（跨链服务位置信息，业务合约信息）。
- (3) 跨链交易数据、交易凭证及数字签名。

### 7.2.1 跨链查询权限要求

跨链查询请求包含跨链发起方、中继链和跨链目标方三个参与者。跨链发起方在进行跨链交易时，先由跨链发起方的业务应用调用中继链代理服务，发起第一阶段的跨链通信。本阶段中，业务应用将预先配置的非对称密钥对对应的公钥地址放入交易凭证中，并通过对应的私钥对协议数据包做数字签名。

中继链代理服务在接收到业务应用的请求后，解析协议中的管道约束信息，并根据交易凭证中业务应用提供的公钥地址，匹配管道搭建时业务应用预留的公钥，该公钥会用于本阶段跨链协议的业务应用身份验证，以及跨链数据的完整性校验。

完成完整性校验的请求方可转发到目标方进行跨链查询。

### 7.2.2 跨链写入权限要求

跨链写入要求系统对发起方进行更严格的认证，除前述的身份验证与跨链数据的完整性验证外，还应包括：

- (1) 中继链代理服务应对管道约束信息进行二次验证，判断本次跨链发起方的权限。
- (2) 中继链代理服务会解析协议中的管道约束信息，并根据交易凭证中跨链发起方提供的公钥地址，匹配管道搭建时跨链发起方预留的公钥。
- (3) 当发起方权限超过目标数据写入权限是，方可成功写入。

### 7.3 协同原则

在多个区块链间进行数据转移，涉及到多省业务系统之间数据的交互，更易出现个人资产、身份数据等隐私信息泄露的问题。协同原则即确保利用可靠的权限管理和授权机制，保障区块链资源的信息安全。在跨链场景下，协同原则宜：

- (1) 将链间的查询与写入的权限控制细化到分区以及资源的具体接口。
- (2) 对新接入的区块链业务系统实时同步和执行来自权限管理合约的权限策略。
- (3) 控制和记录跨链查询、写入的操作，实时保障跨链业务的信息安全。

## 8 链外协同

### 8.1 区块链对外提供访问服务

#### 8.1.1 对外调用接口服务功能要求

对外调用接口服务是一种直接调用形式，使用通用区块链接口从外部直接触发调用。接口类型见表 8.1。

表 8.1 对外调用接口类型

接口类型	描述
------	----

创建接口	将智能合约的创建指令、相关代码和初始化参数传送至智能合约引擎，完成合约实例化。
调用接口	智能合约引擎根据发送者提供的参数，定位智能合约实例，加载合约代码，并执行合约指令。
查询接口	根据指定的智能合约寻址方式，查询智能合约实例的信息，包括合约代码，创建者，内部数据，合约状态等。
升级接口	根据指定的智能合约寻址方式和传入的数据，升级合约代码、内部数据和合约状态等，并将升级操作作为新的交易生成新的智能合约实例。
废止接口	根据指定的智能合约寻址方式，将指定的智能合约实例置为无效。
监管接口	为监管机构提供接口，供其按照监管规则进行操作。
获取环境常量接口	智能合约引擎在运行智能合约代码过程中，区块链系统应为智能合约引擎提供相关数据读取接口，提供的数据应为常量，不能被智能合约引擎修改。
查询日志接口	根据指定的智能合约寻址方式、交易标识和日志文件，查询合约运行时产生的日志。

### 8.1.2 访问控制要求

区块链对外提供访问服务过程中，系统需要接收来自调用方提供的权限验证信息，并将该信息应用于调用过程中的权限判断，安全验证等操作中。权限验证信息宜包括：

- (1) 权限信息（调用方账户信息）
- (2) 业务路由信息（调用方位置信息）。
- (3) 交易数据、凭证及数字签名。

### 8.1.3 联机访问协同原则

区块链对外提供访问服务，与调用方之间应具备协同原则，利用可靠的权限管理和授权机制来保障区块链所提供的接口不被盗用，从而损害区块链资源的安全。协同原则宜：

- (1) 对每个提供的服务接口进行详细的权限控制，限定接口所能访问的区

块链资源。

- (2) 对新调用方进行详尽的权限验证。
- (3) 记录服务调用的操作记录，实时保障业务安全。

## 8.2 区块链系统访问非区块链系统

### 8.2.1 访问控制要求

区块链系统访问非区块链系统时，非区块链系统需要提供相应的访问接口以及对区块链系统访问请求的权限认证手段，保障系统整体业务的安全。非区块链系统需要对系统数据进行加密存储，在认证后提供密钥，供区块链系统进行访问。

### 8.2.2 联机访问协同原则

区块链系统与非区块链系统之间应具备协同原则，利用可靠的权限管理和授权机制来保障区块链系统与非区块链系统之间的数据交互安全。协同原则宜：

- (1) 对区块链系统的访问请求进行权限控制，限定其每次操作所能访问的资源。
- (2) 对系统的每次访问操作进行权限认证，保证加密数据安全。
- (3) 记录系统访问记录，实时保障业务安全。