



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技术
标准

Technical Standards for Toll Road Blockchain

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技术标准

Technical Standards for Toll Road Blockchain Technology

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技术标准》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 7 章,主要包括:1 总则、2 术语与符号、3 基本规定、4 技术要求、5 收费公路联网收费区块链框架和能力、6 收费公路联网收费区块链系统的主要流程、7 数据要求。

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：王炳炯

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.....	9
	4.1 基本要求.....	9
	4.2 服务支持和应用支持方面的技术要求.....	10
	4.3 安全方面的技术要求.....	12
5	收费公路联网收费区块链框架和能力.....	14
	5.1 系统架构.....	14
	5.2 数据流向.....	15
	5.3 基础层.....	15
	5.4 核心层.....	15
	5.5 服务层.....	15
	5.6 应用层.....	16
6	收费公路联网收费区块链系统的主要流程.....	16
	6.1 存证数据上链.....	16
	6.2 存证信息取证.....	17
7	数据要求.....	18
	7.1 上链数据.....	18
	7.2 访问权限.....	19

1 总则

1.0.1 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，制定本标准。

1.0.2 本标准适用于收费公路联网收费系区块链技术相关的产品设计、软件开发、系统部署和应用。

1.0.3 收费公路联网区块链系统建设应积极谨慎地采用新理念、新技术、新设备。

1.0.3 收费公路联网区块链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系统应包含众多参与方,包含省中心以及数十个联网收费站。
- 3.1.4 收费公路联网收费区块链系统应当具备较为出色的记账、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是操作界面相连接。
- 3.1.6 收费公路联网收费区块链系统应保证系统的高安全性,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 收费公路联网收费区块链系统应基于区块链技术与银行等金融机构打通,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。
- 3.1.9 收费公路联网收费区块链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是操作界面相连接。

4 技术要求

4.1 基本要求

公路联网收费系统作为一种区块链技术平台,应需要支持一组与去中心化工作模式相关的基本技术要求:

系统需要支持全部和部分节点参与共识过程,支持公路联网收费系统上的收

费信息存储。

系统需要支持必要的智能合约，并通过智能合约来支持收费信息存储、读取的自动化。

系统需要支持去中心化管理模式下节点管理，包括：身份识别、用户认证、访问鉴权、授权管理和审计等。

除了支持这些基本技术要求外，系统还需要支持服务与应用支持方面和安全方面的技术要求。

4.2 服务支持和应用支持方面的技术要求

1. 接口要求

系统应设计带有身份令牌、签名、时间戳等的消息传播机制，来校验调用请求的合法性，检验数据是否被篡改。系统应避免过期、非法、无效的请求对数据接口以及应用接口进行访问与调用。

同时系统调用接口应支持高级语言 API，以支持系统业务要求的实现与扩展。

(1) 合约调用要求：

- a) 系统应对不同调用方可以使用的智能合约做出区分。
- b) 系统应实现不同智能合约之间的数据隔离，即同一个区块链网络上的多个智能合约业务数据是彼此独立的，一个合约不能直接访问另外一个合约的数据。
- c) 系统也应实现同链方法调用的权限控制，并在开发时以编程接口形式提供给智能合约编写者进行设定。

(2) 合约构建要求：

- a) 在编写智能合约代码时，应符合代码书写规范、逻辑要求等规范性要求。
- b) 在编写智能合约代码时，应使用已经广泛应用的合约语言，宜采用最新的稳定版本。
- c) 涉及收费溯源的智能合约，要求系统向路网中心提交备案材料。
- d) 对已部署智能合约进行升级操作前，要求系统重新提交备案信息。合约备案信息包括智能合约名称，智能合约版本，智能合约序列号，智

能合约访问数据范围等必要信息，写明智能合约的用途。提交方应对项目备案信息的真实性、合法性和完整性负责，并对备案合约进行下述的合约验证过程。

(3) 合约验证要求：

要求系统对智能合约提供必要的审计和验证过程，建议包括安全评估和代码验证两种验证形式。

- a) 安全评估应通过人工阅读文档、源代码、编译器版本等形式，对智能合约业务流程进行安全性的测试和评估。
- b) 代码验证可使用外部权威机构测试。权威机构即具备多种联盟链测试环境的机构。机构应对智能合约的完备性、正确性、适合性和依存性进行软件测试并提供测试报告。
- c) 代码验证也可采用形式化验证报告方式提交，其过程应包括合约制定、形式描述、建模验证、代码生成和一致性测试五个工程部分。

2. 区块链共识要求

(1) 共识可靠性要求：

- a) 系统正常运行节点的请求应能在系统性能所要求的规定时间达成一致的共识。
- b) 系统正常运行节点的请求应能在系统性能所要求的规定时间内达成正确的共识。
- c) 系统正常运行节点的请求应能输出正确结果。建议系统采用确定性共识算法，并能防范确定性算法重放攻击和确定性算法权利压迫攻击。

(2) 共识终局性要求：

- a) 要求区块所有数据均受到密码技术保护。
- b) 要求数据一旦上链，系统应能防止链上交易回滚。
- c) 要求链上记录能通过有限确认块数达到记录稳定状态。

(3) 共识容错性要求：

- a) 要求系统设置正常运行的最大异常节点数，即：部分连接节点网络异常时，系统仍能正常运行。

- b) 要求部分连接节点通信缓慢时，系统仍能正常运行。
 - c) 要求当有理论值范围内的恶意节点对系统发出伪造请求时，系统应能做出正确且一致的响应。
- (4) 共识可审计性要求：
- a) 要求共识记录的内容包括事件时间、内容、发起者信息与事件类型。
 - b) 要求共识记录无法修改、无法删除且共识进程无法单独中断。
 - c) 要求单次共识过程可审计、可监督且不可被篡改。
- (5) 共识可扩展性要求：
- a) 要求系统采用高效可扩展的共识算法，任意不超过理论值的节点退出时不会影响整个系统正常工作。
 - b) 要求系统采用高效可扩展的共识算法，任意不超过理论值的节点新增不会影响整个系统正常工作。

4.3 安全方面的技术要求

1. 密码应用

(1) 密码算法要求

系统中配置和使用的密码算法（包括分组对称加密算法，公钥密码算法、杂凑算法及随机性检测规范）应符合密码国家标准、行业标准的相关要求：

- a) 分组对称加密算法应采用 SM4 密码算法，符合 GB/T 32907。
- b) 公钥密码算法应采用 SM2 椭圆曲线公钥密码算法，符合 GB/T 32918。
- c) 密码杂凑函数应采用 SM3 密码杂凑算法，符合 GB/T 32905。
- d) 随机数生成算法所采用的随机数，符合 GB/T 32915。

(2) 数字签名要求

数字签名和使用要求符合 GB/T 35276、GB/T 35275、GB/T 38635.1 和 GB/T 38635.2。

(3) 密钥管理安全要求

- a) 区块链应用中的身份鉴别密钥、数据加密密钥等应使用通过商用密码检测认证的密码设备或模块对密钥的生成、存储、分发、导入与导出、使用、备份与回复、归档、销毁等环节实现安全管理。

- b) 对区块链节点之间的通信数据加密，以及对区块链节点上存储数据加密的密钥，应通过商用密码检测认证的密码设备或模块将私钥妥善保存。
 - c) 要求密钥进行严格的生命周期管理，不应为永久有效，到达一定的时间周期需进行更换。
- (4) 证书管理要求
- a) 要求证书认证系统和相关的密钥管理系统建设应符合 GB/T 25056、GM/T 0037 和 GM/T 0038。
 - b) 要求数字证书以及 CRL 格式应符合 GB/T 25018
- (5) 数据安全要求
- a) 收费系统的节点和节点之间的数据交换，原则上不应明文传输，宜采用非对称密码技术协商密钥，用对称加密算法进行数据的加密和解密。
 - b) 收费系统各个节点之间、应用端与节点之间可配置安全通道，以保证数据通信的安全。
 - c) 系统应保证传输数据的机密性和完整性。

2. 节点管理

节点是区块链的载体，由安装了特定区块链软件、可连接互联网、拥有可访问的 IP 地址、且可对外提供服务的物理服务器或虚拟服务器组成。

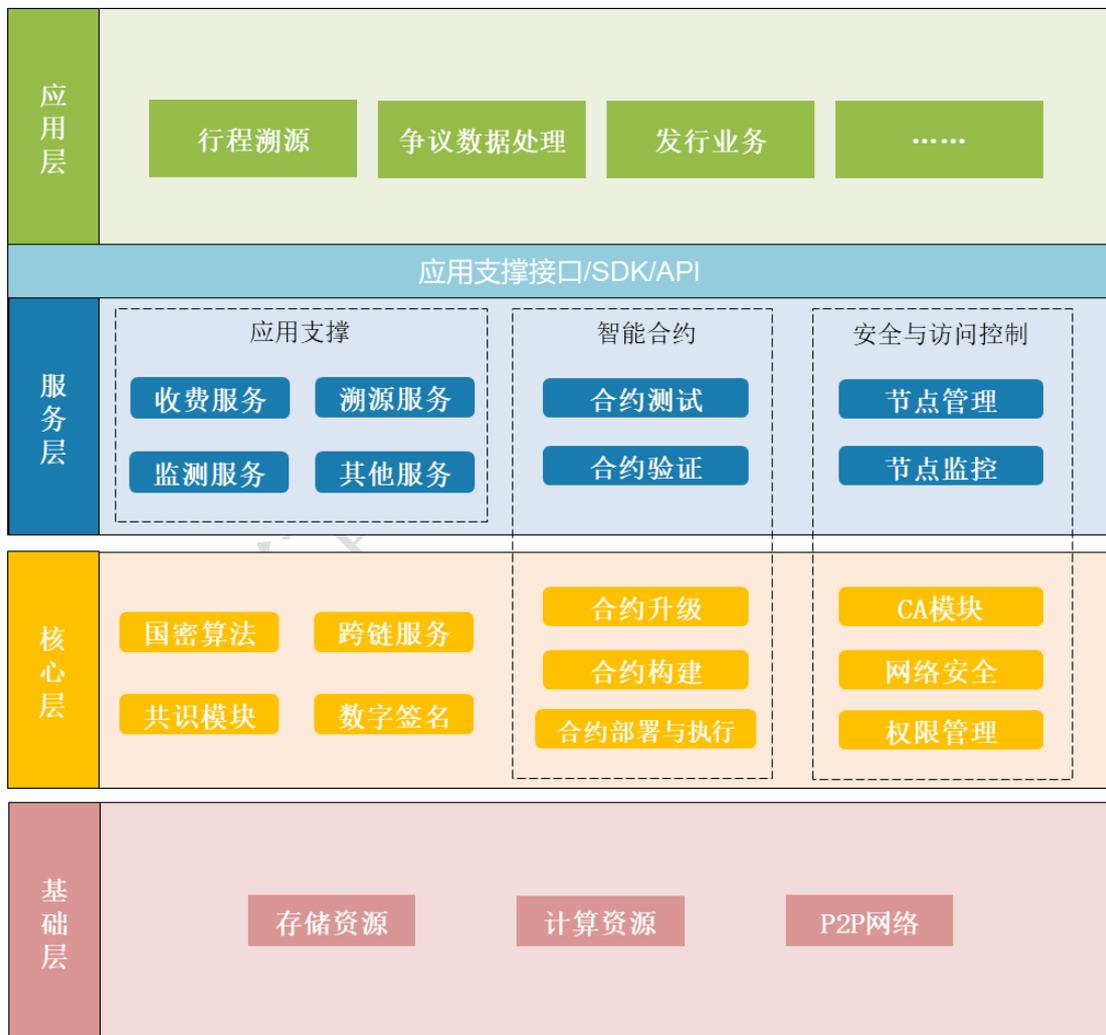
- (1) 准入性要求：
- a) 新节点加入时应向省管理中心提出申请，申请内容包括节点用途，访问数据范围，使用智能合约范围及其他必要申请信息。
 - b) 新节点加入后需要对历史区块进行同步后，方可将新数据上链管理。
- (2) 高可用要求：
- a) 系统应维持 24h 运转，并在规定时间内对新节点加入进行审批。
 - b) 针对不合法节点的申请，系统应能驳回申请，避免恶意节点加入。
 - c) 针对节点退出的情况，系统应能保障应用正常运行，并对退出节点原因进行分析。
- (3) 状态监控要求：

- a) 系统应对链上节点服务器的状态信息进行监控。
- b) 系统应对节点服务能力配置进行监控。
- c) 系统应对节点网络状态进行监控。
- d) 节点应对授权配置管理进行监控。

5 收费公路联网收费区块链框架和能力

5.1 系统架构

基于公路联网收费总体要求以及应用业务要求，初步构建基于功能的公路联



网收费区块链系统架构如图 5.1 所示。

图 5.1 公路联网收费区块链系统架构

5.2 数据流向

由平台设施层产生的数据，经过服务系统传输至基础层进行初步存储。对需要存证的数据，经由核心层的数字签名、摘要算法、加密算法处理后，将摘要信息上链存储。上链存储的数据经过智能合约模块和安全与访问控制模块的控制，为系统提供多种服务，包括：收费服务、溯源服务、检测服务等，并最终支持应用层的行程溯源、争议数据处理等业务。

5.3 基础层

包含计算资源、存储资源和网络资源，该层提供了区块链系统所需要的运行环境。可以充分结合 5G、云计算、大数据、物联网等新兴技术和系统搭建支撑平台运行的基础设施，为平台的存储、计算和网络传输提供技术支撑。

5.4 核心层

提供底层共识平台基础功能的实现，包含六个方面：

- ① 安全与访问控制：主要包括 CA 模块、基础的权限管理和网络安全等。
- ② 共识模块：主要包含具备可靠性、终局性、容错性、可审计性和可扩展性的共识算法模块。
- ③ 国密算法：包含 SM2 算法、SM3 算法、SM4 算法。
- ④ 智能合约：包含智能合约的构建、升级及调用模块。
- ⑤ 跨链服务：包含为区块链提供跨链支持的功能模块。
- ⑥ 数字签名：包含使用国密算法进行数字签名的模块。

5.5 服务层

该层为业务的实现应用层提供支撑，包括应用支撑、智能合约验证、安全访问与控制三部分。

- ① 应用支撑包括收费服务、溯源服务、检测服务等合约实现，充分支撑已有上层业务的实现。
- ② 智能合约验证部分包括对已构建智能合约的测试和验证，确保智能合约

的部署满足完备性、正确性、适合性和依存性，为用户数据的隐私提供保护。

- ③ 安全与访问控制支持节点管理和监控，可保证节点进入和节点状态可管可控，满足系统的安全与隐私保护需求。

同时服务层提供应用支撑服务接口/SDK/API，可同应用服务系统进行对接和继承。

5.6 应用层

包含公路联网收费的各种应用和服务，可利用区块链技术的防篡改、可溯源、高可信等特性开展各类创新业务。

6 收费公路联网收费区块链系统的主要流程

存证信息上链、取证与核验的主要流程如图 6.1 所示：

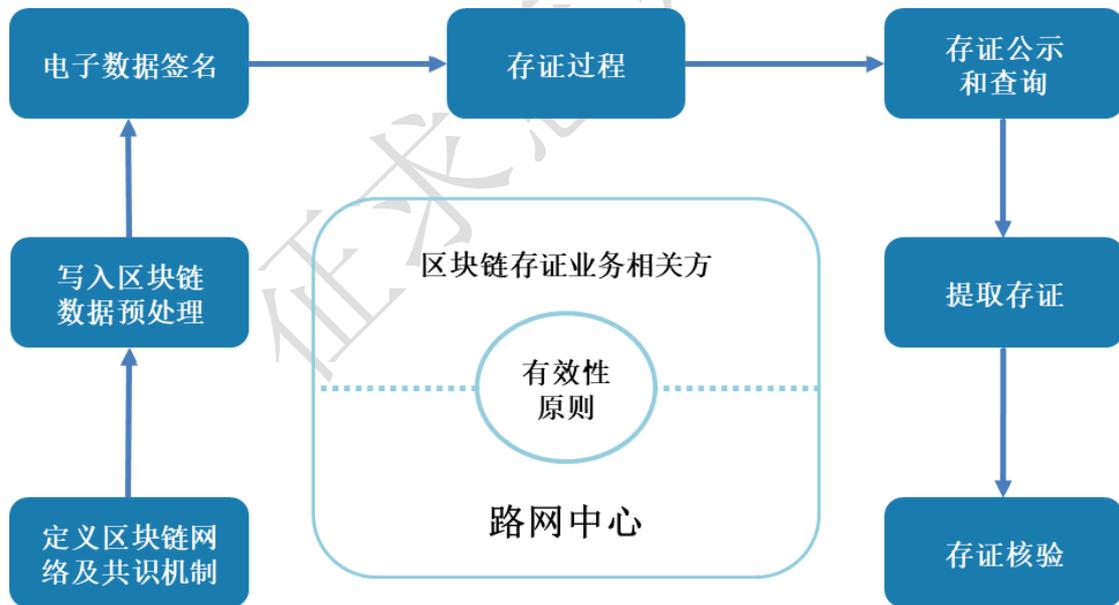


图 6.1 公路联网收费系统存证主要流程

6.1 存证数据上链

6.1.1 定义区块链网络及共识过程

在建立存证系统时，可按需要定义或选择区块链网络的共识机制。系统定义

的共识机制应满足上文中关于服务支持和应用支持方面的技术要求。

6.1.2 写入区块链数据预处理

写入区块链数据预处理时宜：

- a) 检查区块链系统外电子数据满足存证要求。
- b) 检查电子数据的内容是否符合法律法规要求；
- c) 检查电子数据的隐私内容是否已脱敏，是否涉及其他隐私内容。
- d) 对电子数据相关信息进行有效性验证。

6.1.3 电子数据签名

对存证内容做电子数据签名时：

- a) 宜使用合法授权的身份数字证书。
- b) 用户不宜使用被确认泄露或因其他原因失效的私钥。
- c) 用户宜使用本人的私钥进行数据签名。
- d) 已签名的数据应能在区块链网络中验证。

6.1.4 存证过程

存证过程中宜：

- a) 确保电子数据生成、收集、存储、传输所依赖的计算机系统的硬件、软件环境安全可靠。
- b) 明确电子数据的存储、介质保管的方式和手段。
- c) 通过节点向区块链存证系统发起电子数据存证请求进行存证。

6.2 存证信息取证

6.2.1 存证查询

存证数据可利用多种方式进行查询，确保所有省中心可查询公示信息：

- a) 查询可采用网站或公共接口方式。
- b) 查询等功能应体现真实的存证数据，并可通过区块链网络中的节点进行

查询验证。

- c) 可直接使用区块数据查询进行数据验证。

6.2.2 提取存证

提取的存证信息应从区块链网络中直接获取，提取存证时宜：

- a) 确保取证过程所依赖的计算机系统的硬件、软件环境安全可靠。
- b) 提取过程可重现，且提取过程的记录是连续的。
- c) 取证后的出证信息包括原始存证信息、存证参与者身份信息、存证时间信息、必要的数据传输网络地址信息、出证信息及其他必要信息。

7 数据要求

7.1 上链数据

上链数据应与业务场景相对应，满足交易对账和争议处理的证据文件要求。证据文件应准确、完整、详实、有效。文件格式规范清晰，满足业务处理需要，能够精准佐证与该笔追偿协调关联关系和所证明的具体处理意见。

7.1.1 交易对账

交易对账工作主要核对联网收费过程中通行费应收未收交易，建议满足以下数据摘要上链存证：

- a) ETC、CPC 卡进出口通行记录：包括交易编号、入出类型、同行介质类型、介质编码。
- b) 车牌识别记录：包括收费站车牌识别信息、门架车牌识别信息。
- c) 门架交易记录：包含计费交易编号等。
- d) 车辆抓拍照片：应能清楚显示车牌号、交易时间、交易地点等关键信息。
- e) 车辆信息：包括收费车型、车种、重量等。
- f) 车道日志：应包含卡号、OBU 号、交易时间、交易地点、交易金额（包括应收金额、实际收费金额、优惠金额等）及特情记录等关键信息，日志文件应为车辆出口收费完整记录，不能为数据库文件须转换为文字格

式。日志文件不单独作为证据文件支撑，应匹配关联相应的图像或录像证实交易真实存在且有效。

- g) 卡状态传输历史信息截图，应包含 ETC 卡号、节点时间等关键信息。
- h) 系统截图：上传交易时间记录的系统截图，应包含 ETC 卡号、OBU 号、车牌号、交易时间、节点时间等关键信息。
- i) 还应包括现场查验货物图片、免费车辆证明等，能够证明与车辆的关联关系。。

7.1.2 争议处理

为满足争议处理要求，建议满足以下数据摘要上链存证：

- a) 特情支付数据编号：包括出口车道编号、交易批次号、流水号。
- b) 通行介质类型：1 标记 OBU，2 标记 CPC 卡，3 标记纸券，4 标记 M1 卡，9 标记无通行介质。
- c) 收费车辆车牌号码及颜色：格式为车牌号_车牌颜色，例：京 A12345_1
- d) 特情类型：包括 OBU 电量低、OBU 拆卸、OBU 过期、OBU 未启用、OBU 无卡、OBU 在状态名单里、OBU 已锁、OBU 发行方无效等情况，以 1-40 分别标记。

7.2 访问权限

系统应根据各节点对不同交易数据的可见权限，将部分或全部节点划分在一个或多个分区内；同一分区内部对于交易数据完全可见，不同分区之间对于交易数据不可见。

7.2.1 部网中心节点

部网中心节点在联盟链中拥有最高权限，节点可使用联盟链上所有智能合约，以便于访问各分链上的交易收费数据。

7.2.2 省中心节点

省中心节点在本省联盟链中拥有最高权限，节点可使用联盟链上所有智能合约，以便于访问各收费站提交上链的存证数据。

7.2.3 省收费站节点

省收费站节点在本省联盟链中拥有较低权限，节点可使用联盟链上部分智能合约，仅可用于上传收费存证数据，跨链数据调用等请求应提交省中心后进行。

征求意见稿