

团体标准

T/CESA XXXX—202X

基于区块链的碳排放管理系统技术要求

Blockchain and distributed ledger technologies — Specification for trusted carbon emission

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

已授权的专利证明材料为专利证书复印件或扉页，已公开但尚未授权的专利申请证明材料为专利公开通知书复印件或扉页，未公开的专利申请的证明材料为专利申请号和申请日期。

202X-XX- XX 发布

202X-XX- XX 实施

中国电子工业标准化技术协会 发布



版权保护文件

版权所有归属于该标准的发布机构，除非有其他规定，否则未经许可，此发行物及其章节不得以其他形式或任何手段进行复制、再版或使用，包括电子版，影印件，或发布在互联网及内部网络等。使用许可可于发布机构获取。

目次

前 言 IV

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 符号和缩略语 1

5 总体架构 2

6 支撑层 2

 6.1 基础设施 2

 6.2 共识机制 2

 6.3 智能合约 3

 6.4 摘要 3

 6.5 账本记录 3

 6.6 密码服务 3

 6.7 节点管理 3

7 核心层 4

 7.1 可信身份 4

 7.2 可信数据 4

8 应用层 5

 8.1 业务应用 5

9 碳排放数据计算方法要求 5

 9.1 通则 6

 9.2 计算周期 6

 9.3 计算边界识别 6

 9.4 计算方法 6

附录 A（资料性）碳排放可信数据算法 7

附录 B（资料性）主要能源碳排放因子参考值..... 9

附录 C（资料性）能源消耗量参与区块链交易的数据格式..... 11

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。

本文件由广东电网有限责任公司广州供电局提出。

本文件由中国电子工业标准化技术协会区块链工作委员会归口。

本文件起草单位： 。

本文件主要起草人： 。

基于区块链的碳排放管理系统技术要求

1 范围

本文件确立了运用区块链技术对碳排放数据可信性管理要求和计算方法，给出了区块链数据管理平台架构支撑层、核心层、应用层的要求。

本文件适用于：

- a) 为能源提供方和温室气体排放单位运用区块链技术对碳排放数据进行管理计算提供参考依据；
- b) 为区块链碳排放可信数据管理系统建设方提供指导；
- c) 为能源监管部门的监督管理提供技术支撑。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

GB/T 25069和ISO 22739界定的以及下列术语和定义适用于本文件。

3.1

碳排放 carbon emission

碳排放单位在核算边界内生产、活动和服务过程中各个环节产生的所有二氧化碳排放量，以二氧化碳当量的形式表示。

[来源：GB/T 32150-2015, 3.7]

3.2

碳排放因子 carbon emission factor

将能源与材料消耗量与二氧化碳排放相对应的系数，用于量化不同阶段相关活动的碳排放。

3.3

数据元 data element

由一组属性规定其定义、标识、表示和允许值的数据单元。

[来源：GB/T 18391.1-2009 3.3.8]

3.4

数据类型 datatype

一些可区分的值的集合，这种区别由这些值的性质以及对这些值的运算所表征。

[来源：GB/T 18391.1-2009 3.3.11]

4 缩略语

下列缩略语适用于本文件。

RSA ——RSA加密算法(RSA algorithm)

SM2 ——SM2椭圆曲线公钥密码算法(SM2 algorithm)
SM3 ——SM3杂凑算法(SM3 algorithm)
SM9 ——商密九号算法(SM9 algorithm)

5 总体架构

基于区块链的可信碳排放数据管理平台包括支撑层、核心层、应用层见图 1，其中：

- a) 支撑层应具备碳排放数据的存证/取证、存证数据查询、数据核验以及存储、计算和网络能力；
- b) 核心层包括可信身份模块与可信数据模块；
- c) 应用层包括对接外部系统进行碳认证、碳核查、碳交易及政府部门进行数据监管等；

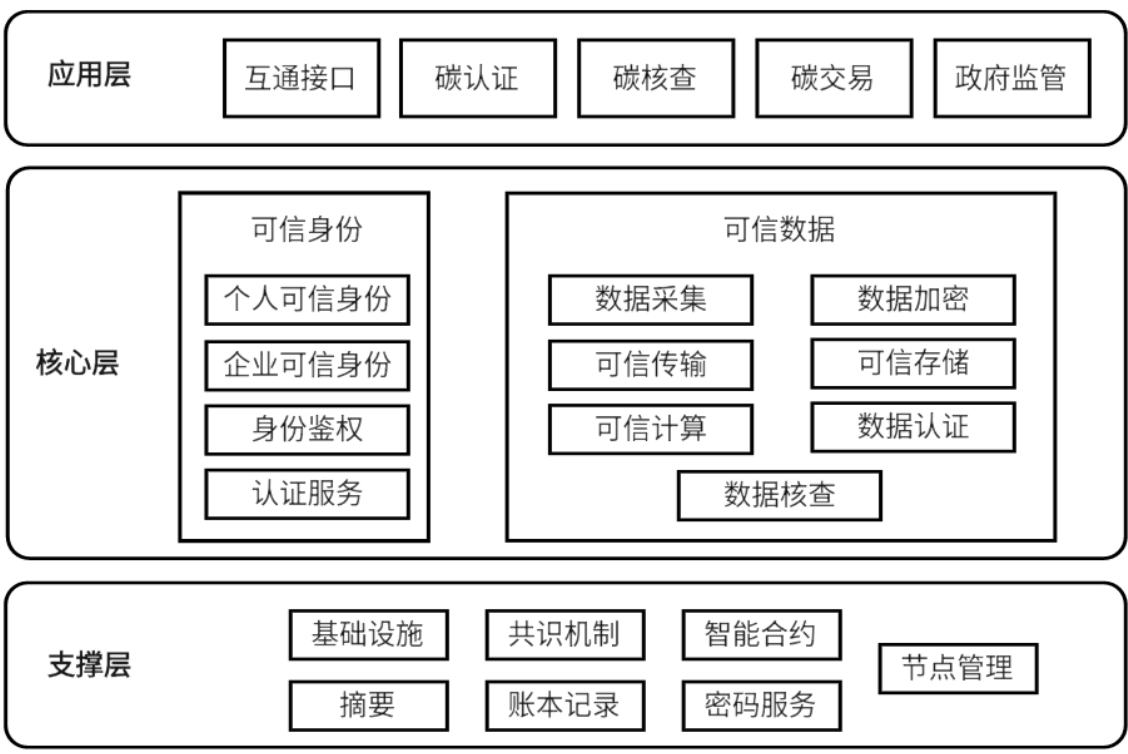


图1 基于区块链的可信碳排放数据管理平台总体架构图

6 支撑层

6.1 基础设施

基础设施为区块链系统提供正常运行所需要的环境和基础组件，应符合：

- a) 采用分布式对等网络协议组织区块链网络中的节点，并使用点对点通信协议完成信息交换以支撑上层功能；
- b) 各区块链节点部署存储组件，为支撑层提供稳定的数据写入与查询功能；
- c) 计算资源被各区块链节点调用，对支撑层提供运行环境支持。

6.2 共识机制

共识机制功能组件通过特定的共识算法，完成区块链节点的共识过程。其功能应包括：

- a) 多节点参与共识和验证，应能在节点在线、离线、网络调整等情况下，不停止系统服务替换共

识协议、切换共识机制并达成新的全网共识；

- b) 独立节点对区块链网络提交的相关信息进行有效性验证；
- c) 应保持每个节点更新账本状态写操作的一致性，并保证每个节点账本的最终状态一致；
- d) 应能识别且拒绝未经共识确认的新增或修改信息；
- e) 具备一定的容错性，包括物理或网络故障等非恶意错误、节点遭受非法控制等恶意错误。

6.3 智能合约

智能合约功能组件支持在预设规则前提下，根据特定输入产生特定结果。智能合约的编制应符合：

- a) 智能合约源代码应符合安全编码规范要求，应具备正确的操作逻辑，保证智能合约的正确性和安全性；
- b) 智能合约的执行应具备一致性，即在任意节点上的执行结果应完全相同；
- c) 可提供虚拟机或虚拟化技术在内的运行载体支持；
- d) 对于与区块链系统外部数据进行交互的智能合约，外部数据源不影响区块链系统的整体运行；
- e) 应提供智能合约在线全生命周期管理，包括合约编写、编译、部署、调用、升级及冻结等；
- f) 防止对合约内容进行篡改；
- g) 多方共识下的合约内容升级。

6.4 摘要

摘要功能组件应符合：

- a) 不可逆性，已知函数值的情况下，恢复函数输入的难度不小于破译密码服务中加密算法的难度；
- b) 可验证性，同样输入必然得到同样输出，且函数值的正确性可被独立验证；
- c) 具备抗撞击能力，不同输入得出同样输出的概率极小。

6.5 账本记录

账本记录功能组件泛指区块链中分布式数据的存储机制，通过不同节点对账本的共同记录与维护，形成区块链系统中数据的公共管理、防篡改、可信任的机制。其功能应满足：

- a) 账本数据的持久化存储；
- b) 多节点拥有延时完整数据；
- c) 向节点提供已授权数据；
- d) 确保有相同账本记录的各节点的数据一致性。

6.6 密码服务

密码服务功能组件包括以下功能：

- a) 宜支持国际主流加密算法，如 AES256 等对称加密算法和 RSA、ECC 等非对称加密算法；
- b) 宜支持我国主流商密算法，如 SM3、SM4 等对称加密算法和 SM2、SM9 等非对称加密算法；
- c) 使用可信第三方提供的时间戳，保证时间戳的可信赖性和不可抵赖性；
- d) 应具备明确的密钥管理方案，确保区块链底层安全机制的正常运行；
- e) 加密算法应具备抵御破解的能力，应定期审核加密算法的安全性。

6.7 节点管理

节点管理组件支持对区块链节点的信息查询、管理和控制。其功能应包括：

- a) 提供区块链节点服务器的状态信息查询服务；
- b) 提供区块链节点服务器的启动与关闭服务；
- c) 提供区块链节点服务器的节点服务能力配置；
- d) 提供区块链节点服务器网络连接状态监控服务；

- e) 提供区块链节点准入准出配置、节点事务处理和账本查询授权配置。

7 核心层

7.1 可信身份

本标准针对能源监管部门、能源提供方和温室气体排放单位制定，企业最终管理依托法定代表人或企业授权人等个人主体，本节明确了个人可信身份的要求。

7.1.1 个人可信身份

个人可信身份数据的采集、注册和鉴权包括下列要求：

- a) 碳排放数据管理相关方应设置可信的身份认证机构，负责身份注册，并接受相关监管部门的督查与紧急干预；
- b) 应实现读卡、OCR 识别等方式采集证件数据信息；
- c) 应实现平台录入、用户授权、第三方身份关联等方式采集手机号数据；
- d) 应实现采用摄像头拍摄设备采集人像数据；
- e) 应依照相关法律法规，征得用户同意，收集、使用、存储、传输和销毁用户身份信息；
- f) 用户身份信息的收集应遵循最小化原则，仅收集必要的信息；
- g) 应提供第三方身份数据库核验功能；
- h) 应实现个人用户证件数据、手机数据、生物特征数据绑定生成个人用户账号；
- i) 应实现数字证书与个人用户账号绑定，封装成个人用户可信身份数据。

注：第三方数据库指国家级权威数据库，例如国家或地方公安部门的电子数字身份库。

7.1.2 企业可信身份

企业可信身份数据的采集、注册和鉴权包括下列要求：

- a) 已完成个人可信身份认证数据、企业证照数据与法定代表人信息数据采集、对公账号信息数据采集；
- b) 应支持系统平台录入方式采集个人可信身份数据；
- c) 应支持系统平台录入、实时 OCR 识别等方式采集企业证照和法定代表人信息；
- d) 应支持系统平台录入方式采集对公账号信息；
- e) 应支持企业信息第三方核验功能，对企业信息真实性进行验证，其中第三方数据库指国家或地方工商部门管理的电子营业执照数据库；
- f) 应实现企业用户证照数据、法定代表人数据、联系数据绑定生成企业用户账号；
- g) 应实现数字证书与企业用户账号绑定，封装成企业用户可信身份数据。

7.2 可信数据

可信数据负责保障平台上数据的真实性、安全性和可靠性，通过使用数据加密技术实现数据的安全上链、存储和授权。可信数据包括数据采集、数据脱敏、数据加密、可信传输、可信存储、数据认证与数据核查，并具备下列能力：

- a) 数据采集：
 - (1) 应提供多种原始数据获取方法，包括：人工填报、人工导入等人工采集方式，与设备对接、应用系统对接等系统采集方式；
 - (2) 应提供多种数据实时性方案，包括：数据实时上链，数据非实时上链；
 - (3) 应通过对数据的有效预处理，保证数据查询、授权数据修改、数据恢复等操作的效率。
- b) 数据脱敏：

- (1) 个人数据脱敏应包括证件信息、手机号信息、口令数据、笔迹数据等敏感信息；
- (2) 企业数据脱敏应包括证照信息、法定代表人信息、联系人信息和对公账户信息。
- c) 数据加密：
 - (1) 应实现采用相关标准的系列非对称加密算法（如 RSA、SM2）、散列算法（如 MD5、SM3、SHA256）、对称加密算法（如 DES、SM4）等；
 - (2) 应支持数据传输或存储时数据报文、数据文件加密；
 - (3) 敏感账本数据的保护密钥和账本数据本身应分开保存，且保护密钥应支持存放于安全的密码模块中。
- d) 可信传输：
 - (1) 应支持 SSL、TLS 等协议；
 - (2) 应支持数据重传机制；
 - (3) 应支持传输数据校验机制；
 - (4) 应支持传输监控告警；
 - (5) 应支持传输对象身份校验机制，包括口令、权限、源地址。
- e) 可信存储：
 - (1) 应保证账本数据在产生、传输、存储、下载等过程中不被非授权方式篡改或损坏；
 - (2) 对账本数据的写入和修改，须经各节点达成共识，以保证各节点的数据一致性，当出现数据分叉时，应存在可用规则进行数据选择；
 - (3) 应保证账本数据在系统中具有冗余性，以防止因单个节点的失效而造成总账本的数据丢失；
 - (4) 应提供账本数据备份方法，当出现账本数据的丢失或损毁的故障节点数量不超过理论阈值时，系统仍能恢复完整的账本数据；
 - (5) 应提供账本数据访问审计，审计记录应包括访问时间、位置、访问节点身份标识、访问内容等相关信息；
 - (6) 应提供账本数据修改审计，审计记录应包括数据修改时间、访问位置、修改节点身份标识、改数据内容等相关信息；
 - (7) 审计记录不仅包括数据变更成功的记录，还应包括数据变更失败的记录；
 - (8) 审计记录应写入区块链账本，以保证安全审计的可靠性。
- f) 数据认证：能源提供方应对温室气体排放单位提交的碳排放相关能源数据进行认证及校验。
- g) 数据核查：能源监管机构应对温室气体排放单位提交的碳排放相关数据进行核查以验证其真实性。

8 应用层

8.1 业务应用

业务应用应具备以下能力：

- a) 外部业务系统对可信碳排放数据管理平台的功能调用，业务场景包括碳认证、碳核查、碳交易及政府监管等；
- b) 通过互联接口，实现可信碳排放数据管理平台与第三方系统间用户互通、业务互通、数据互通等要求；
- c) 接口服务应灵活部署，负载均衡，独立部署，支持 http/https、restful、websocket、webservice 等常见接口类型；
- d) 所有与外部系统间的接口调用应进行链路跟踪，监控服务调用的过程并保留日志。

9 碳排放数据计算方法要求

9.1 通则

基于区块链的碳排放可信数据计算方法应符合以下要求：

- a) 相关性，二氧化碳排放量数据和计算方法的选择应真实反映温室气体排放单位二氧化碳排放情况，满足企业管理、报告、制定减排计划的需求。二氧化碳排放量的分项计算应清晰表明各工艺过程排放量及相互之间的关系；
- b) 一致性，企业应使用统一的计量单位计算二氧化碳排放量，使有关二氧化碳排放信息能够进行比较；
示例：碳排放计量结果以吨二氧化碳(t-CO₂)为单位表示，其他温室气体计量结果以吨二氧化碳当量(t-CO₂e)表示。
- c) 准确性，企业应选择适当的计算方法保障二氧化碳排放计算的准确性和精度；
- d) 透明性，企业应给出有明确的、可核查的二氧化碳排放计算过程，对计算方法及数据来源给出说明；
- e) 真实性，企业应保障计算数据的真实性，能真实反映实际排放情况。

9.2 计算周期

碳排放数据计算以自然月或自然年为统计周期，在进行碳排放计算前先确定计算周期，自然年周期数据可由自然月数据汇总得到。

9.3 计算边界识别

碳排放数据计算边界按照企业法人（或视同法人）的厂界区域和运营控制范围确定，一般确认方式如下：

- a) 组织边界可通过企业成立时间、规模、经营范围、资产状况、主要产品种类、产量和产能，主要生产装置、工序及其数量和运行情况，以及厂区平面分布图和组织架构图等进行辅助识别；
- b) 企业组织边界识别结果原则上应与能源统计报表制度中规定统计边界基本一致；
- c) 工业企业应对组织边界内工业生产活动的二氧化碳排放相关数据进行监测、核算与报告，非工业生产活动的二氧化碳排放相关数据不进行核算；
- d) 单位的组织边界指单位法人的运营控制范围。单位组织边界可通过了解单位的成立时间、规模、业务范围、资产状况、组织架构图等进行辅助识别；
- e) 组织边界识别时，集团法人、跨省分支机构等情况的处理方式，边界变化的处理方式和存在业务外包情况按照有关碳排放核查指南处理。

9.4 计算方法

碳排放数据计算方法参照附录A，应按下列步骤进行：

- a) 界定碳排放单元过程；
- b) 采集碳排放单元过程的活动水平数据；
- c) 采集碳排放单元过程的相关碳排放因子（主要能源碳排放因子参考值参照附录B）；
- d) 按照本文件规定的方法核算建筑碳排放量；
- e) 按照规定对外发布计量结果。

注：碳排放因子指将能源与材料消耗量与二氧化碳排放相对应的系数，用于量化不同阶段相关活动的碳排放。

附 录 A
(资料性)
碳排放可信数据算法

概述

企业(单位)根据自身是否有测定燃料的元素碳含量选取计算燃烧产生的二氧化碳排放量。本文件的碳排放仅包括企业直接燃烧和间接排放过程。

热值法

当企业(单位)没有实测燃料的元素碳含量时,按公式(1)计算:

$$AE_{com} = \sum (AD_{j,l} \times Q_{j,l} \times EF_{j,l} \times 10^{-6}) \dots\dots\dots (1)$$

式中:

- AE_{com} ——燃烧产生的二氧化碳排放量,单位为吨二氧化碳(t-CO₂);
- AD ——活动数据,即燃料使用量,单位为吨(t)或万立方米(10⁴m³);
- Q ——低位发热量,单位为兆焦耳/吨燃料(MJ/t)或兆焦耳/万立方米燃气(MJ/10⁴m³);

实测碳含量法

当企业(单位)有实测燃料的元素碳含量或者通过测定燃料成分而计算获得燃料的含碳质量分数时,按公式(2)计算:

$$AE_{com} = \sum (AD_{j,l} \times C_{mj,l} \times \frac{44}{12}) \dots\dots\dots (2)$$

式中:

- AE_{com} ——燃烧产生的二氧化碳排放量,单位为吨二氧化碳(t-CO₂);
- AD ——活动数据,即燃料使用量,单位为吨(t)或万立方米(10⁴m³);
- C_m ——单位质量或体积燃料的碳含量,单位为吨碳/吨燃料(t-C/t)或吨碳/万立方米燃气(t-C/10⁴m³);

消耗外购热力产生的排放

以质量为单位计量的热水和蒸汽按公式(3)、(4)和(5)进行转换计算。

$$AD_{外购热} = AD_{热水} + AD_{蒸汽} \dots\dots\dots (3)$$

式中:

$AD_{热水}$ ——热水所含的热量,单位为吉焦(GJ),按公式(4)计算;

$$AD_{热水} = Ma_w \times (T_w - 20) \times 4.1868 \times 10^{-3} \dots\dots\dots (4)$$

式中:

- Ma_w ——热水的质量,单位为吨(t);
- T_w ——热水的温度,单位为摄氏度(℃);

$$AD_{蒸汽} = Ma_{st} \times (En_{st} - 83.74) \times 10^{-3} \dots\dots\dots (5)$$

式中:

$AD_{蒸汽}$ ——蒸汽所含的热量,单位为吉焦(GJ);

Ma_{st} ——蒸汽的质量，单位为吨(t)；

En_{st} ——蒸汽所对应的温度、压力下每千克蒸汽的热焓，单位为千焦每千克(kJ/kg)。

外购电力、热力间接二氧化碳排放计算方法

外购电力、热力间接二氧化碳排放按计算使用公式(6)计算；

$$AE_e = \sum AD_{e,k} \times EF_e \quad (6)$$

式中：

AE_e ——外购电力、热力导致的间接排放量，单位为吨二氧化碳(t-CO₂)；

AD_e ——活动数据，即净外购电力、热力的使用量，单位为万千瓦时(104kWh)或百万千焦(GJ)；

EF_e ——外购电力、热力排放因子，单位为吨二氧化碳/万千瓦时(t-CO₂/104kWh)或吨二氧化碳百万千焦(t-CO₂/GJ)；

附 录 A
(资料性)
主要能源碳排放因子参考值

主要能源碳排放因子参考值见表B. 1。

表 B. 1 主要能源碳排放因子参考值

排放范围	能源名称	单位	低位发热量	单位热值碳含量	排放因子
直接排放	无烟煤	吨	27631	27. 4	100. 47
	炼焦烟煤	吨	28200	26. 1	95. 7
	一般烟煤	吨	23736	26. 1	95. 7
	褐煤	吨	15250	28	102. 67
	煤制品	吨	17460	33. 6	123. 2
	型煤	吨	20515	33. 6	123. 2
	水煤浆	吨	20905	33. 6	123. 2
	焦炭	吨	28446	29. 5	108. 17
	其他焦化产品	吨	43961	29. 5	108. 17
	原油	吨	42620	20. 1	73. 7
	汽油	吨	44800	18. 9	69. 3
	煤油	吨	44750	19. 6	71. 87
	柴油	吨	43330	20. 2	74. 07
	燃料油	吨	41816	21. 1	77. 37
	煤焦油	吨	33453	26	95. 33
	液化石油气（LPG）	吨	50179	17. 2	63. 07
	液化天然气（LNG）	吨	51498	15. 3	56. 1
	天然气液体（NGL）	吨	46900	17. 2	63. 07
	炼厂干气	吨	46055	18. 2	66. 73
	石脑油	吨	45010	20	73. 33
	润滑油	吨	41449	20	73. 33
	石蜡	吨	39998	20. 3	74. 43
	石油沥青	吨	38999	22	80. 67
	石油焦	吨	32500	27. 5	100. 83
	石化原料油	吨	46400	20	73. 33
	其他石油制品	吨	41030	20	73. 33
	天然气	吨	389310	15. 3	56. 1
	煤矿瓦斯气	吨	167260	15. 3	56. 1
	焦炉煤气	吨	179810	13. 58	49. 79
	高炉煤气	吨	37630	84	308
	转炉煤气	吨	79539	55	201. 67
	其他煤气	吨	202218	12. 2	44. 73
	发生炉煤气	吨	52270	12. 2	44. 73

排放范围	能源名称	单位	低位发热量	单位热值碳含量	排放因子
	水煤气	吨	104540	12.2	44.73
	粗苯	吨	41816	22.7	83.23
	煤矸石	吨	8373	26.61	97.59
	城市固体垃圾	吨	7954	9	33
	工业废料	吨	12558	35.1	128.7
	废油	吨	40200	20.18	73.99
	废轮胎	吨	31400	4.64	17.01
	塑料	吨	50800	20.45	74.98
	废溶剂	吨	51500	16.15	59.22
	废皮革	吨	29000	6	22
	废玻璃钢	吨	32600	22.64	83.01
间接排放	电力排放因子（吨二氧化碳/万千瓦时）			6.379	
	热力排放因子（吨二氧化碳/百万千焦）			0.1	

附 录 C
(资料性)

能源消耗量参与区块链交易的数据格式

能源消耗量参与区块链交易的数据格式见表C. 1。

表 C. 1 能源消耗量数据格式

名称	字段	必填	类型	长度
能源购入企业名称	epeName	是	字符型	<=64 字节
能源购入企业统一信用代码	epeCreditCode	是	字符型	18 字节
能源卖出企业名称	eseName	是	字符型	<=64 字节
能源卖出企业统一信用代码	eseCreditCode	是	字符型	18 字节
交易能源类型	energyTradedType	是	字符型	<=20 字节
交易能源数量	energyTradedQuantity	是	字符型	<=10 字节
交易能源单位	energyTradedUnit	是	字符型	<=10 字节
交易能源时间	energyTradedTime	是	日期型	10 字节
能源发票代码 (电子票据)	energyInvoiceCode	是	字符型	<=20 字节
能源发票号码 (电子票据)	energyInvoiceNumber	是	字符型	<=20 字节

参 考 文 献

- [1]GB 17167-2006 用能单位能源计量器具配备和管理通则
- [2]GB/T 25069-2010 信息安全技术术语
- [3]GB/T 32150-2015 工业企业温室气体排放核算和报告通则
- [4]GB/T 34945-2017 信息技术数据溯源描述模型
- [5]GB/T 51366-2019 建筑碳排放计算标准
- [6]T/CESA 6002—2017 区块链 数据格式规范
- [7] DB11/T 1370-2016 低碳企业评价技术导则
- [8] DB11/T 1559-2018 碳排放管理体系实施指南
- [9]ISO 22739:2020 信息技术 区块链和分布式记账技术 术语 (Blockchain and distributed ledger technologies - Vocabulary)

