ICS 35.020
CCS L 70

T/GDEIIA

团　体　标　准

T/GDEIIA xx—2023

能源区块链系统实施指南

Energy Blockchain System Implementation Guide

（征求意见稿）

2023－xx－xx 发布　　2023－xx－xx 实施

广东省电子信息行业协会　　发布

目　次

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。

本文件不涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广东电网有限责任公司提出。

本文件由广东省电子信息行业协会归口。

本文件起草单位：广东电网有限责任公司、南方电网数字企业科技（广东）有限公司、湖南天河国云科技有限公司、南方电网人工智能科技有限公司、广东天河国云科技有限公司

本文件主要起草人：陈军、裴求根、伍江瑶、郑灶贤、吴欣欣、尹海波、姚昱旻、孔曼、杨能、杨伟、徐驰、肖晶、欧阳昌忠、魏来

本文件为首次发布。

能源区块链系统实施指南

1 范围

本文件规定了能源区块链系统的实施过程。

本文件适用于：

a）为能源区块链的实施提供正确的指引；

b）统一对能源区块链技术实施的认识，为应用能源区块链服务提供指导性意见；

c）降低能源区块链技术应用风险，提升能源区块链技术应用效果。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

JR/T 0193-2020 区块链技术金融应用 评估规则

GB/T 25069-2022 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1 区块链（Blockchain）

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。

[来源：JR/T 0193-2020]

3.2 能源区块链（Energy Blockchain）

能源区块链主要指区块链技术在能源物联网领域的应用，能源系统中的各个能源结点通过区块链技术加密存储能源交易信息数据，利用共识机制完成分布式能源决策，然后利用智能合约机制完成能源的自动交易，实现能源交易过程中能量流、信息流和价值流的有效衔接。

3.3 对称密码算法（Symmetric Cryptographic Algorithm）

加密和解密采用同一密钥的密码算法。

[来源：GB/T 25069-2022]

3.4 SM-算法（Shang Min - Algorithm）

为了保障商用密码的安全性，国家商用密码管理办公室制定了一系列密码标准，包括 SM1（SCB2）、SM2、SM3、SM4 等算法。其中 SM1 是分组密码算法，常用于系列芯片、智能 IC 卡等；SM2 是椭圆曲线公钥密码算法，常用于加解密、数字签名等；SM3 是杂凑算法，常用于数字签名和验证；SM4 是对称算法，常用于无线局域网产品。

3.5 ECC-算法（Elliptic Curves Cryptography Algorithm）

基于椭圆曲线密码算法系列，将椭圆曲线密码算法与其他算法组合形成具备不同功能的密码算法。包括 ECDSA 数字签名算法、ECIES 公钥加密算法等。ECDSA 是 ECC 算法和 DSA 算法的组合，用于数字签名；ECIES 是一种基于椭圆曲线集成的密钥交换+对称加密+消息验证码算法体系。

3.6 工作量证明机制（PoW, Proof of Work）

是一种对应服务与资源滥用、或是拒绝服务攻击的经济对策。一般要求用户进行一些耗时适当的复杂运算，并且答案能被服务方快速验算，以此耗用的时间、设备与能源做为担保成本，以确保服务与资源是被真正的需求所使用。

3.7 权威证明机制（PoA, Proof of Authority）

是一种基于声誉的共识算法，通过基于身份权益（Identity as a Stake）的共识机制，提供更快的 交易速度。

3.8 联盟链（Consortium Blockchain）

联盟链采用半去中心化的结构，即参与验证交易的共识过程依赖于一组预定义的网络节点，确定能源交易将被验证。联盟链是能源公司之间的业务用途密切相关，能源公司借助区块链技术提高其业务运作的效率。这是因为联盟链拥有常规区块链的所有内置安全措施，但同时允许对网络进行更大程度的控制。

3.9 应用程序接口（API, Application Programming Interface）

是一种计算接口，它定义多个软件中介之间的交互，以及可以进行的调用（call）或请求（request）的种类。

3.10 远程过程调用(RPC, Remote Procedure Call）

是一种计算机通信协议。该协议允许运行于一台计算机的程序调用另一个地址空间的子程序，而程序员就像调用本地程序一样，无需额外地为这个交互作用编程。

3.11 公开密钥基础设施(PKI, Public Key Infrastructure）

是一组由硬件、软件、参与者、管理政策与流程组成的基础架构，其目的在于创造、管理、分配、使用、存储以及撤销数字证书。

3.12 证书撤销列表(CRL, Certificate revocation list)

证书撤销列表，是尚未到期就被证书颁发机构吊销的数字证书的名单。这些在证书吊销列表中的证书不再会受到信任。

3.13 CA（Certificate Authority）

CA是证书的签发机构，它是公钥基础设施（Public Key Infrastructure，PKI）的核心。CA是负责签发证书、认证证书、管理已颁发证书的机关。

4 技术要求

4.1 密码机制

4.1.1 密码算法

能够应对不同加密场景提供高安全、高效率、灵活配置的密码算法。包括以下密码算法：

a）国产商用密码算法：支持 SM2 数字签名算法、SM2 公钥加密算法、SM4 对称加密算法以及 SM3 哈希算法等国产商用密码算法。

b）国际标准密码算法：支持 ECDSA 数字签名算法、ECIES 公钥加密算法、AES 对称加密算法、SHA 系列哈希算法等主流国际标准密码算法。

c）安全可控的定制密码算法：为满足不同场景的安全需求，区块链平台支持定制安全可控的私有化密码算法的能力，包括：数字签名算法、公钥加密算法、对称加密算法和哈希算法等。

d）其他主流密码算法：支持其他主流密码算法。

4.1.2 密钥管理

主要负责对区块链平台所使用的密码算法的密钥进行管理。

a）密钥安全存储：将不同密码方案不同时期的密钥与区块链平台的模块建立一一映射关系，安全存储在特定的页表中。

b）密钥安全更新：为了有效提高平台的安全性，所有使用的密钥需要定期更新。

c）密钥安全读写：在平台初始化以及发生密钥更新时，为平台内部需要使用密码算法的模块提供密钥读写服务。

4.2 共识机制

4.2.1 工作量证明机制

工作量证明机制（PoW），即对于工作量的证明，是生成要加入到区块链中的一笔新的交易信息(即新区块)时必须满足的要求。在基于工作量证明机制构建的区块链网络中，节点通过计算随机哈希散列的数值解争夺记账权，求得正确的数值解以生成区块的能力是节点算力的具体表现。 PoW 共识机制十分简单，可以给部署带来很大的便捷，且具有高安全性，因为破坏系统需要投入极大的成本，但可能会造成一定程度的资源浪费，网络性能不高。具体包含以下功能：

a）PoW 区块生成：节点按照 PoW 预定规则，生成合法区块，并广播至网络中。

b）PoW 区块验证：按照 PoW 预定规则，接收到新区块的其他节点验证新区块的有效性，若验证通过，则将新区块添加到自己的链上。

4.2.2 权威证明机制

权威证明机制（PoA）是一种高效的共识机制。依赖于可信验证者 (Validator)，只有 Validator 可以生成区块，Validator 的添加和删除需要所有 Validator 的投票完成。不需要浪费算力以获取生成区块的资格，极大地提高了交易吞吐量。具体包含以下功能：

a）可信验证者添加：根据预设规则以及可信验证者的投票，添加新的可信验证者。

b）可信验证者删除：根据预设规则以及可信验证者的投票，删除可信验证者。

c）POA 区块生成：按照 POA 的预定规则，Validator 收集交易并生成合法区块，并广播到网络中。

d）POA 区块验证：按照 POA 的预定规则，接收到新区块的其他节点验证新区块的有效性，若验证通过，则将新区块添加到自己的链上。

e）自主设计的共识区块生成：按照预定规则，生成合法区块，并广播到网络中。

f）自主设计的共识区块验证：按照预定规则，接收到新区块的其他节点验证新区块的有效性，若验证通过，则将新区块添加到自己的链上。

4.3 智能合约

4.3.1 数据存储

智能合约的数据存储在底层数据库，每个智能合约具有逻辑上的独立存储区，采用数据结构组织每个智能合约的数据，并将树根的哈希值存储到合约账户的账户状态中写入区块链。支持的数据类型包括值类型、引用类型以及映射。

4.3.2 数据更新

通过调用智能合约可以对不同类型的数据进行操作，并更新数据。在智能合约的开发过程中可以进行权限控制，只有通过权限验证的调用才可以更改数据。底层数据库的数据更改后，计算更新后的树根哈希值，并将更新后的树根哈希值存入账户状态写入区块链。

4.3.3 基本运算

智能合约为不同的数据类型提供了基本运算，方便智能合约开发过程中对数据的操作，主要包括的运算类型包括：

a）逻辑运算：逻辑非（!）、逻辑与（&&）、逻辑或（||）；

b）比较运算：小于等于（<=）、小于（<）、等于（==）、不等于（!=）、大于等于（>=）、大于（>）；

c）位运算：按位与（&）、按位或（|）、异或（^）、取反（~）；

d）算数运算：加（+）、减（-）、一元运算+、一元运算-、乘（*）、除（/）、取余（%）、幂（**）、左位移（<<）、右位移（>>）；

4.3.4 事件监听

事件是日志基础设施提供的一个接口，事件可以用来做操作记录，存储为日志。如果监听了某事件，当事件发生时，会进行回调。

4.3.5 合约库

合约库与普通的合约类似，目的是在一个指定的地址，且仅部署一次，支持其他合约调用，实现代码复用，在降低开发者开发难度时，提供高质量的合约代码，减少代码漏洞的出现。

4.4 数据处理

4.4.1 数据上链

a）上链数据预处理：对预备上链的数据进行必要的数据块分割、类型转化，便于后续的存储；

b）存储结果返回：将预处理后的数据存储至区块链中，并返回数据在区块链中存储的地址，包括区块号等。

4.4.2 数据查询

a）数据查询请求解析：获取查询请求并解析查询请求中指定待查询数据在区块链中存储的地址；

b）数据查询结果返回：执行查询步骤，并返回查询结果。

4.4.3 数据下载

a）数据下载请求解析：获取查询请求并解析下载请求，包括需要下载的区块号、数据分块（在默克尔树快速校验中，只需下载部 2 分数据分块）等；

b）数据下载结果返回： 执行下载步骤，并返回下载结果。

4.4.4 完整性校验

a）数据校验请求解析：获取校验请求并解析校验请求，包括待校验的数据及其所在的区块号；

b）数据校验结果发布：计算待校验数据所在区块的默克尔根，并与区块头中存储的默克尔根进行对比；若不相等，则输出校验数据有误，否则，输出校验数据正确。

4.5 日志管理

4.5.1 日志记录

a）平台运行日志：记录平台运行中的重要信息，包括平台的启动、运行状况、异常情况等。

b）应用管理日志：记录平台在应用管理中的重要行为，包括 API 管理、流量控制、应用认证、监控告警等操作。

c）用户管理日志：记录平台在用户管理中的重要行为，包括证书管理、身份认证、访问控制、权限管理等操作。

d）节点管理日志：记录平台在节点管理中的重要行为，包括节点配置、节点初始化、添加、删除、接口设置等操作。

e）数据管理日志：记录平台在数据管理中的重要行为，包括数据上链、查询、下载及校验等操作。

f）监督管理日志：记录平台在监督管理中的重要行为，包括用户登录、管理员及普通用户对平台公告的操作等。

4.5.2 分类日志查询

支持分类查询日志记录，包括系统日志、应用管理日志、用户管理日志、节点管理日志、数据管理日志、监督管理日志。

4.5.3 日志分析

按类别统计各类日志的数量，并用图表的形式进行展示。

4.6 应用用户管理

4.6.1 API 管理

用于管理应用的 API 接口，包括创建、配置、修改、调试、查询和删除操作。

a）创建：用于创建 API 接口，创建 API 前，用户需要先创建服务，每个 API 都有自己归属的服务。

b）配置：用于配置 API 接口，包括 API 基础信息配置、前端配置、后端配置和响应配置。

c）修改：用于修改 API 接口，对已经配置的 API 接口进行编辑修改，修改后的 API 需要重新发布 API 所在的服务到对应环境方能生效。

d）调试：用于调试 API 接口。用户在配置完成后可调用此接口进行调试，无需等到发布后走正式的调用流程。

e）查询：用于查询 API 接口，可查询 API 接口列表、接口信息、使用计划详情等。

f）删除：用于删除 API 接口。

4.6.2 服务管理

用于管理应用的服务，包括创建、修改、查询和删除操作。一个服务内包含多个相关联的 API。

a）创建：用于创建服务。API 网关使用的最大单元为服务，每个服务中可创建多个 API 接口。每个服务有一个默认域名供客户调用，用户也可绑定自定义域名到此服务中。

b）修改：用于修改服务的相关信息。服务创建后，服务的名称、描述和服务类型均可被修改。

c）查询：用于查询服务的相关信息，包括服务列表、服务环境列表、服务版本、服务详情等。

d）删除：用于删除某个服务。

4.6.3 发布管理

用于管理应用的发布，包括发布、环境切换、版本切换、发布后访问和下线操作。

a）发布：用于服务的发布。在完成服务内 API 的配置后，即可进行发布。

b）环境切换：用于选择需要发布服务的环境。可提供测试、预发布、发布等多种环境用以部署外接应用的 API。

a）版本切换：用于提供切换版本的能力。
b）发布后访问：用于服务发布后的 API 访问。通过服务的子域名或自定义域名可访问 API。
c）下线：用于发布的撤销。服务下线后，外部将无法访问到此环境上的服务。

4.6.4 流量控制

用于管理应用的流量控制。根据外接应用自身的业务需求对 API 服务进行流量配置，提供秒级的请求过滤与控制，避免突发高流量导致后端服务过载，用以保障业务的稳定性。

4.6.5 认证服务

用于给应用提供严格的认证服务。为了保护 API 的安全，避免恶意访问、未授权访问、应用漏洞、黑客攻击等导致的数据损失、资产损失，此模块提供多种 API 认证方式和防护策略。外接应用使用 API 网关提供的密钥进行认证，没有被授予密钥的应用无法调用 API。

4.6.6 监控告警

用于应用的监控告警。实时监控 API 调用情况，包括请求数、流量使用、响应时间、错误异常等。对自身 API 的分析提供方便可靠的数据依据。以便 API 的后期迭代与维护，提高效率。

4.6.7 PKI 认证服务消息分发

由 PKI 认证服务向区块链控制台提供认证相关的展示信息，如 PKI 证书的颁发情况等。

5 区块链全生命周期管理

5.1 联盟组织管理

5.1.1 联盟管理

用于对联盟的管理，包括如下功能：跨域组网-联盟方申请、跨域组网-邀请联盟方加入等功能。

5.1.2 多组织管理

用于对组织的管理。包括如下功能：组织新增、组织修改、组织动态加入网络、组织删除、组织查询、组织管理操作审核等功能。

5.2 节点管理

节点管理模块包括节点的基础信息配置、初始化、添加、删除以及接口设置。用户可使用此模块对区块链网络中的节点进行操作，用以满足自身业务的需求。

5.2.1 基础配置

用于提供区块链基础的配置信息，管理配置信息的添加、修改和查询操作。

配置信息：包括网络配置信息和节点配置信息。网络配置信息包含区块链网络的 ID、共识机制、节点个数、燃料限制和所在地域等。节点配置信息包含区块链节点的 IP、端口和密钥信息等。

添加：用于添加配置信息。节点初始化前，需要配置区块链网络信息和节点信息。节点添加前，需要配置节点信息。

修改：用于修改节点配置信息。可修改指定节点的 IP、端口。

查询：用于查询配置信息。

5.2.2 节点初始化

用于区块链节点的初始化操作。通过自定义的网络配置信息和节点配置信息创建新的区块链网络以及服务。

5.2.3 节点添加

用于添加新的区块链节点。包括节点配置、节点生成、建立连接。通过配置节点信息，生成节点的公私钥对，手动添加节点，与原有区块链网络中的节点建立连接。

5.2.4 节点删除

用于删除现有区块链网络中的指定节点。

5.2.5 接口权限控制

用于设置节点 RPC 接口的用户名和密码。

5.3 通道管理

用于对通道的管理。包括如下功能：通道新增、出块策略设置、通道修改、通道删除、通道查询、通道管理操作审核等功能。

6 区块链用户管理

6.1 用户证书管理

6.1.1 证书注册

用于证书申请。用户通过提供真实的身份信息和凭证向 CA 申请获得数字证书，CA 根据申请者提供的资料验证其身份。

6.1.2 证书颁发

用于电子证书的颁发。将分发给申请者的公钥与其身份信息绑定，为之签名，形成数字证书颁发给

申请者。

6.1.3 证书撤销

用于电子证书的撤销。当 PKI 中某实体的私钥被泄漏时，泄密私钥对应的公钥证书应被作废。或者如果证书中包含的证书持有者和某组织的关系已经中止，相应的公钥证书也应该被作废。通过发布证书撤销列表 CRL 确保必要时可以废除证书。

6.1.4 证书更新

用于电子证书的更新，包括在密钥泄露时的更新和证书过期后的更新。生成新的密钥和新的证书。

6.2 用户密钥管理

6.2.1 密钥生成与分发

用于密钥的生成与分发。身份认证通过后，生成公私钥对并分发给申请者。

6.2.2 密钥恢复

用于密钥的恢复。允许丢失的或忘记的私钥恢复或激活的协议。

6.3 用户身份管理

6.3.1 身份认证

对接入区块链网络的用户进行身份认证，即验证其是否具备有效的 CA 证书。

6.3.2 访问控制

对不同的用户设置不同的权限，通过颁发不同权限的证书实现。

6.3.3 权限控制

通过设定访问策略，对于拥有不同权限的用户，可以访问不同的内容。

7 区块链平台控制台

7.1 运行状态可视化

提供完备齐全的数据展示屏，通过清晰直观的动态数据图与交互动画展现区块链平台的运行状况及实时性能指标，由以下数据图表构成。

a） 当前区块高度图表：显示当前监控的区块链中最新区块的区块编号，实时反映出区块链网络的更新情况；

b）区块产出间隔图表：展示监控的区块链网络近期产生的区块的间隔时间，以动态数据图表的形式呈现，反映了区块链网络中的共识性能；

c）区块数据可视化：对区块链平台中新产生的区块、操作及账户进行呈现，便于运维人员对平台工作情况及平台数据的监督与管理；

d）平台数据吞吐量可视化：以动态图表的形式呈现区块链平台的操作吞吐量，反映了平台处理数据读写的能力；

e）区块链账户状态可视化：以动态图表的形式展现区块链平台中的活跃账户以及它们所执行的操作，方便运维人员对平台的用户进行监管；

f）区块链智能合约状态可视化：以动态图表的形式展现区块链平台中活跃的智能合约程序以及它们的调用情况，方便运维人员对平台上运行的智能合约进行监管；

g）负载均衡状态信息可视化：具体包括负载均衡节点运行状况监控信息、负载均衡节点资源利用率监控信息以及负载均衡系统请求处理状况图表的可视化展示。

7.2 节点状态可视化

方便运维管理人员实时观察区块链网络节点的运行情况，并据此对区块链网络的节点进行管理配置，具体包含以下功能：

a）节点运行情况监控：展示区块链网络中节点程序的运行情况，包括节点的上线情况、节点同步状态、节点数据处理状态等信息；

b）节点网络状况监控：展示区块链网络中节点的网络连接情况，包括节点的邻节点信息、网络延迟、传输数据量等信息；

c）节点资源利用率监控：展示区块链网络节点所在主机系统的资源利用情况，包括处理器、内存、磁盘及网络等资源信息。

7.3 区块链数据浏览

为运维人员及管理人员提供区块链网络中数据的浏览与查询接口，具体包括以下部分功能：

a）区块链用户数据图表：查看区块链平台中的注册用户列表、查看注册用户的详细信息，包括用户身份、用户证书、用户操作等；

b）区块链操作信息图表：查看区块链平台中的操作列表、查看操作的详细信息，包括操作的参与方、操作业务数据及签名等；

c）区块链应用统计图表：查看区块链平台接入的应用情况，浏览接入应用的详细信息及接口使用情况。

8 监督管理

8.1 监督员登录

为监督员提供登录接口，并在登录后跳转监督员管理功能界面，提供对平台的监督管理窗口。

8.2 平台运行状况查看

以可视化的方式展示平台运行健康状态、平台硬件资源利用率，平台访问量等信息。

8.3 应用支撑情况查看

以可视化的方式展示平台支撑的应用情况，包括应用规模、应用类别、地域分布等。

8.4 安全问题处理情况查看

以统计图表的方式展示平台面临过的安全问题，以及对重大安全问题的响应及时程度。

8.5 平台实时运行状态查看

以直观的动态图像的方式向展示平台当前运行的状态，包括当前采用的共识机制、密码算法，在线节点数量及其分布状况，区块数量产生速率等信息。

9 存储管理

9.1 数据维护

数据维护主要包括授权数据的修改、删除以及授权操作的记录。具体功能描述如下所示：

a）授权数据修改：在管理部门的授权下，可对区块链平台的链上哈希值进行修改。

b）授权数据删除：在管理部门的授权下，对错误或无效数据进行删除。

c）授权操作记录：将授权的数据修改和删除等关键操作进行记录，便于后续审计。

9.2 映射关系维护

将企业数据库数据与区块链数据建立映射关系，在企业数据库内存储原始数据，在链上保存对应数据的标识（哈希值），实现协同存储。合理映射关系的建立，依赖于安全技术（哈希、签名）的选择。映射关系是后续数据的查询、删改等各项操作，数据完整性审计和数据监管的基础。

9.3 数据目录维护

建立映射数据目录，便于后续的数据查询。

9.4 数据一致性校核

校验企业数据库中的原始数据与区块链平台的链上哈希值是否一致，当发生非法篡改时，能够在一定时间范围内发现篡改行为并发出提醒。

10 负载均衡

10.1 心跳检测

由负载均衡服务器定时向每个节点发送心跳包，检测节点在线状态。

10.2 消息队列

10.2.1 区块链服务消息分发

由区块链服务向区块链控制台提供区块链相关的展示信息，如实时区块信息、账户信息、智能合约信息等。

10.2.2 负载均衡服务消息分发

由负载均衡服务向区块链控制台提供系统调度相关的信息，如节点资源占用情况、数据负载情况等。

10.3 节点状态统计

各个节点主动向负载均衡服务器推送机器当前运行状态，如内存、硬盘等。

10.4 节点负载均衡

通过负载均衡算法进行流量分发，使得多个区块链节点分担应用、用户请求，消除单点故障，提升系统可用性。

10.5 数据负载均衡

能源区块链平台采用区块链和多个数据库协同存储,将数据在多个节点上冗余存储,分担数据请求,提升数据可用性。

10.6 服务负载均衡

与信息系统对接则需要API接口或定制接口。