



广州供电局 2026 年数字技术平台适 应性改造项目（区块链平台广州边缘 节点升级-电政通跨链数据核验）技 术规范书

广东电网有限责任公司广州供电局

2026 年 3 月



目录

一、 总则	1
1.1 依据的标准和规范	1
二、 项目概况	2
2.1 项目要求	2
2.2 项目背景	3
2.3 建设目标	3
2.4 建设范围	5
2.5 项目保质期	5
三、 项目内容与要求	6
3.1 项目准备工作	6
3.2 项目管理要求	6
3.3 项目参与人员要求	7
3.4 实施保证	8
3.5 项目功能需求与设计要求	11
3.6 技术要求	15
3.7 自主可控要求	17
3.8 技术标准与规范引用	18
3.9 安全技术方案	19
3.10 性能要求	27
3.11 实施工作要求	27
3.12 测试要求	30
3.13 项目转分包要求	30
四、 项目实施 技术联络组	31
招标人验收组	31
4.1 时间进度安排	31
4.2 技术联络	31
4.3 验收	31
4.4 培训	32
4.5 项目交付项	33
4.6 知识产权要求	34
五、 服务方案	34
六、 服务团队及服务能力	34
（一）团队规模	34
（二）团队能力要求	35
（三）项目负责人要求	35
七、 进度计划及保障措施	35

八、 服务质量保证措施 36

九、 服务承诺36

十、 售后服务和技术支持 36

 10.1 质保期服务内容 36

 10.2 技术服务承诺 38

十一、 响应要求及服务评价标准38

 11.1 事件响应服务要求 38

 11.2 服务水平评价 40

十二、 主要条款/参数优异性表格响应表 45

十三、 技术条款/技术参数点对点应答表 46

十四、 服务团队优异性表 47

十五、 一般服务团队条款/参数应答表 47

十六、 评价申辩48

十七、 违约责任48

 17.1 合同终止条款48

 17.2 评分扣款说明49

十八、 效力说明49

一、总则

1.1 依据的标准和规范

项目建设应遵循国家标准、电力行业标准、工信部、南方电网公司、广东电网公司、广州供电局颁布的标准（包括标准、制度、规范、管理办法）开展本项目工作，本项目所有成果应符合上述标准要求。所用的标准必须是最新版本，如果这些标准的内容有矛盾时，应按照最高标准的条款执行或按双方协商同意的标准或条款执行。

相关标准和文件包括但不限于：

1. 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
2. 《“数据要素×”三年行动计划（2024-2026年）》
3. 《可信数据空间发展行动计划（2024—2028年）》
4. 《关于完善数据流通安全治理 更好促进数据要素市场化价值化的实施方案》
5. 《中国南方电网有限责任公司发展战略纲要》
6. 《中国南方电网有限责任公司信息化职能战略》
7. 《中国南方电网有限责任公司信息化项目建设管理细则》
8. 《南方电网公司数字南网建设技术架构管控工作指引（试行）》
9. 《中国南方电网有限责任公司软硬件平台架构和资源分配指导意见》
10. 《关于进一步加强公司信息化项目和数据管理工作的通知》
11. 《中国南方电网有限责任公司数据资产管理办法》
12. 《中国南方电网有限责任公司数据资产管理行动计划》
13. 《中国南方电网有限责任公司数据模型管理细则》
14. 《中国南方电网有限责任公司数据应用管理细则》
15. 《中国南方电网有限责任公司数据共享开放管理细则》
16. 《中国南方电网有限责任公司信息安全保障体系》
17. 《中国南方电网有限责任公司网络安全管理办法》
18. 《中国南方电网有限责任公司网络安全和数字化工作管理规定》
19. 《南方电网公司信息化项目预算编制与计算方法（20204年修订版）》

- 20. GB/T 43572-2023 《区块链和分布式记账技术 术语》
- 21. GB/T 43575-2023 《区块链和分布式记账技术 系统测试规范》
- 22. GB/T 43579-2023 《区块链和分布式记账技术 智能合约生命周期管理》
- 23. GB/T 43580-2023 《技术规范区块链和分布式记账技术 存证通用服务指南》
- 24. GB/T 43582-2023 《区块链和分布式记账技术 应用程序接口 中间件技术指南》
- 25. GB/T 42752-2023 《区块链和分布式记账技术 参考架构》
- 26. GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》
- 27. T/GZBIA 001 - 2025 《政务区块链建设规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日**
- 28. T/GZBIA 002 - 2025 《政务区块链技术安全规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日**
- 29. T/GZBIA 003 - 2025 《政务区块链跨链数据格式规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日**

二、项目概况

2.1 项目要求

本项目属于升级改造项目，投标方有如下经验优先：

1. 具有政务区块链平台相关项目经验优先。
2. 完全理解区块链在能源管理与政务服务跨链对接的开发和业务，完全理解南方电网广州供电局区块链相关业务和管理制度，能够提供有效的区块链技术应用在跨领域、跨部门业务的解决方案，完全理解广州政务区块链“穗智链”的技术和运行，并具备应用上链支撑服务能力。
3. 全面掌握项目的整体概况，对项目背景、现状、目标、建设范围与内容及重难点具备精准的理解；在此基础上，深入熟悉建设内容，准确理解相关业务需求及特点；并能系统分析项目建设中的难点与痛点，提出具有创新性的关

键业务解决方案。

2.2 项目背景

在当前国家全面推进数据要素市场化配置的战略背景下，以推动数据要素高水平应用为主线，以推进数据要素协同优化、复用增效、融合创新作用发挥为重点，强化场景需求牵引，带动数据要素高质量供给、合规高效流通，培育新产业、新模式、新动能，充分实现数据要素价值。能源行业作为数据密集型关键领域，亟需构建可信、安全、高效的数据要素流通基础设施，开展具备数据要素乘数效应的典型场景创新应用。区块链技术是数据要素流通的基础支撑技术之一，通过分布式架构和可信数据体系，解决数据流通与共享中的安全、合规与信任问题，保障数据流通安全、激活数据要素价值。

广州供电局作为南方电网在广州的重要运营主体，是国家区块链创新应用综合性试点项目的特色试点单位，在南方电网区块链基础上，已建有广州供电局区块链平台，上链绿电溯源、虚拟电厂等链上应用场景，并持有“南方能源行业可信数据空间”牌照，成功入选国家行业可信数据空间创新发展试点（能源）。目前，广州供电局已开展与广州政务区块链--“穗智链”的跨链对接，且“穗智链”已开展与广州互联网法院的“网通法链”司法区块链平台、广州交易集团的“广智链”区块链平台等行业联盟链的跨链互通，在数据要素领域的区块链可信数据基础设施生态已经初步形成。

作为南方电网的服务窗口，广州供电局率先响应国家战略决策，围绕可信数据空间建设和数字经济发展的需求，以区块链技术应用为抓手，发挥能源行业数字化引领作用。为此，亟待对现有广州供电局区块链平台能力进行优化提升与应用拓展，重点建设区块链可信数据交换平台，开展“区块链+”、“电力数据要素×”的典型场景创新应用，并通过与广州政务区块链“穗智链”的跨链互操作，重点推进跨领域、跨行业的业务协作与数据流通，探索数据要素流通和价值实现的创新路径。

2.3 建设目标

基于南方电网区块链广州供电局区块链平台的建设基础，及前期已实现的与广州政务区块链“穗智链”的跨链对接，在广州供电局区块链平台上，优化提升边缘节点的跨链数据存证、验证、流通能力，开发“电政通”标准化功能模块，

建设区块链可信数据交换平台，开展“能源区块链+”的创新应用，打造“区块链电力数据要素×”的典型场景标杆；以区块链可信数据基础设施为支撑，实现开放型“电政通”跨链数据核验和“电务+政务”一网通办业务协作，打通广州供电局区块链平台与广州政务区块链“穗智链”的跨链互操作、数据流通共享，实现能源行业与政务服务跨领域的数据要素流通和价值激活。具体目标包括：

（1）升级区块链平台广州边缘节点。优化跨链网关，通过集成基于轻客户端验证的非侵入式核验机制，并遵循广州政务区块链“穗智链”跨链接口规范，提升跨链数据核验、传递和流通等互操作能力，强化区块链可信数据基础设施对业务系统的服务支撑；完善链上服务基础功能模块体系，提升平台的稳定性、扩展性与业务承载能力，为后续创新应用的规模化落地提供可靠的技术底座。

（2）建设区块链可信数据交换平台。基于广州供电局区块链平台建设可信数据交换平台，与南方能源行业可信数据空间、广州政务区块链“穗智链”构建基于区块链的数据流通道，实现跨平台数据的可信采集、整合与汇聚，支持数据的可信核验、流通、共享与可追溯存证，为数据要素及数据资产的安全流通与价值释放提供区块链基础支撑，同时为后续多场景创新应用的持续拓展预留标准化接口能力。

（3）构建与广州政务区块链“穗智链”的标准化对接功能模块“电政通”。基于现有跨链互通基础，对接广州政务区块链“穗智链”已认证的区块链合规服务组件（包括电子证照、电子签章等），构建南方电网区块链广州供电局区块链平台与广州政务区块链“穗智链”公共服务体系之间的标准化对接通道，纳入区块链可信数据交换平台服务资源库，为后续业务应用的自主开发提供标准化调用支撑，降低重复建设成本。

（4）打造区块链+电力惠民服务典型应用场景。围绕电力数据+政务数据的共享互认，开展“区块链电力数据要素×”创新应用，依托区块链可信数据交换平台，建设民政低保户优惠场景的链上服务能力，支持外部权威资质认定数据的可信接入与链上核验，实现惠民服务申请、资质核验、服务核销全流程的数据上链管理，提升惠民服务的可信度与办理效率，打造区块链惠民服务典型应用场景，为后续同类业务场景的链上化改造积累可复用技术路径与实施规范。

2.4 建设范围

业务范围：围绕构建安全、高效、可信的电力数据要素化基础设施，促进与政务数据的跨链协同与价值释放的核心目标，升级区块链平台广州边缘节点，优化可信跨链互操作，确保南方电网区块链与广州政务区块链“穗智链”间数据交互的安全、准确、可追溯。

建设单位：广州供电局数字运营中心

应用范围：广州供电局数字运营中心

建设范围：本项目属于广州供电局区块链平台的升级改造和应用拓展项目，建设范围包括升级区块链平台广州边缘节点、建设区块链可信数据交换平台、支持电政通跨链数据核验、研究民政低保户优惠“区块链数据要素×”创新应用等相关功能开发及实施工作，为广州供电局南方能源行业可信数据空间与广州政务区块链“穗智链”提供跨链互操作、业务协作与数据流通等服务。

2.5 项目保质期

本项目的保质期为系统建设竣工验收合格之日起一年，保质期内投标人需免费为项目提供包含以下系统支持服务：

➤ 电话热线服务

配备有经验的售后工程师接听客服电话，及时响应招标人提出的系统问题。

要求响应时间范围为 7×24 小时。响应速度为 10 分钟以内。

➤ 远程支持

对于客服电话解答不了的问题，由售后工程师通过远程网络连线至主机进行远程支持。

要求响应时间范围为：7×24 小时。响应速度 30 分钟以内。

➤ 现场服务

对出现不能远程解决的问题，或在系统的运行环境不完全成熟的条件下，需要提供售后工程师的上门服务，现场解决问题。

要求响应时间范围为：7×24 小时，响应速度 2 小时内到达现场。

三、项目内容与要求

3.1 项目准备工作

投标人在项目启动后优先开展准备工作，熟悉招标人在业务管理、信息技术管理及信息化项目管控方面的制度与标准规范，消化、吸收、评估、完善前期需求分析与概要设计阶段成果，对本项目涉及的外部平台接口环境（包括但不限于跨链通道现状、公共服务平台接口申请流程及技术规范）开展充分调研，形成书面调研报告。在上述工作基础上，制定本项目管理章程。

3.2 项目管理要求

（一）投标人实施人员须按照招标人考勤要求出勤，不得迟到、早退、无故旷工。

（二）协助招标人完成合同各阶段支付所需的验收确认工作，按节点及时提交符合要求的验收材料。

（三）合同签订之日起 15 个工作日内，在工作方案基础上制定总体实施方案，细化项目具体实施计划、工作职责与分工，明确各阶段工作里程碑、交付物清单及外部协调节点，由双方确认后遵照执行。工作计划须单独列明涉及外部平台接口申请、跨链对接等外部依赖事项的预计周期与应对预案。

（四）合同签订后，投标人须配合招标人组织召开项目启动会，完成项目组织架构确认、计划宣贯及资源协调等启动事项。

（五）合同履约期间，定期组织项目例会，频率不低于每两周一次，重要外部对接节点前后须增加专项沟通会。向招标人汇报当前阶段工作结果及外部协调进展，接收招标人反馈意见并及时调整，确保项目持续符合承诺指标要求。

（六）在需求分析、系统设计、系统上线等 3 个关键阶段节点，开展阶段检查，形成检查总结报告并落实整改措施，编制阶段性总结报告并组织汇报。

（七）各阶段交付物提交前，投标人须完成交付物自查工作，形成报告，经招标人确认后方可提交正式交付。招标人保留对交付物内容和质量进行审查评审的权利，投标人须根据审查意见在规定时限内完成修改。

（八）合同履约期间，投标人须按时提交周报、月报及问题分析报告，

确保项目信息透明可追溯。

（九）凡涉及外部对接的工作节点，投标人须提前向招标人报告推进进展，如因外部原因导致节点延误，须在延误发生后 3 个工作日内提交书面说明及调整方案，经招标人确认后方可调整相关里程碑节点。

（十）投标人须积极协助招标人推进与外部平台的接口申请及对接协调工作，及时同步外部平台的技术要求、申请进展及潜在风险。外部协调工作中产生的沟通记录、申请材料、接口文档等均须归档并移交招标人留存。

（十一）合同履约期间若出现管理缺陷或管理事故，投标人须按照招标人出具的整改通知书要求，在规定时限内完成整改并提交整改报告。

3.3 项目参与人员要求

（一）人员配置要求

投标人须根据项目实施需要配置足够的项目团队成员，项目组总人数不得少于 5 人，并须指定 1 名项目经理作为甲乙双方对接责任人，并提供不少于 1 名项目应急人员，在项目经理临时无法到位情况下由应急人员顶替。投标人需在合同签订后 15 个工作日内向招标人提供项目组成员名单。

人员名单如下表所示。

序号	姓名	职务	本项目分工	备注
1				
2				
3				
4				

以下表格每人一份。资质需提供证书复印件。

姓名		角色	
身份证号码			
资质			
工作经历			

（二）人员安全审查要求

鉴于本项目涉及甲方业务数据及可信数据交换平台建设，投标人所有参与项目实施的人员须配合招标人完成身份核验与安全背景审查，审查通过后

方可接触甲方相关系统及数据资源。招标人有权对审查不通过的人员提出更换要求，投标人须在收到通知后 5 个工作日内完成替换。

（三）人员变更要求

项目实施期间，项目组成员如需调整或更换，投标人须提前提交书面申请并加盖公章，经招标人书面同意后方可执行。替换人员的能力水平不得低于原人员，并须重新完成安全审查流程。

（四）离场权限管理要求

项目实施期间及项目结束后，投标人须配合招标人及时完成离场人员的系统账号注销、门禁权限回收及数据访问权限清除工作。人员离场须由招标人相关负责人确认签字，投标人不得自行操作权限变更。

（五）运维团队要求

项目验收后，投标人须与招标人组成联合运维团队，明确双方在日常运维、故障响应、版本更新等方面的职责分工，并在验收前提交运维方案及人员配置计划，经招标人审核确认后执行。

（六）项目实施环境要求

本项目包含内部系统改造与外部平台对接两类工作。其中，涉及甲方内部系统接入、数据访问及安全敏感操作的工作内容，投标人须在招标人指定工作场地开展，并满足以下要求：

1. 工作场地须位于招标人现场车程 30 分钟以内，确保响应及时性。
2. 工作场地须具备正常办公所需的网络、电话、客户终端等基础设施，具备工作能力；场地、设备及网络接入等相关费用由投标人自行承担。
3. 内部系统部署及联调工作需在招标人提供的专属工作场地（位于招标人现场步行 5 分钟以内）内完成，以确保信息安全管理要求。

涉及外部平台对接、跨链接口申请及第三方协调的工作内容，不受上述驻场要求约束，但投标人须保持与招标人的实时沟通响应能力，相关工作进展须按项目管理要求及时报告。

3.4 实施保证

（一）组织保证

1. 招标人有权对投标人拟派参与本项目的人员进行面试，面试通过后

方可进场；

2. 项目团队须包含项目经理、项目实施人员、区块链技术支持人员及后台应急支持人员，各角色职责须在项目管理章程中明确；

3. 投标人进场时须向招标人提交完整的项目组成员名单及个人资质证明材料；

4. 项目实施期间，投标人须保证团队人员稳定性，人员变动须经招标人书面同意后方可执行。

（二）质量保证

1. 投标人须在项目启动阶段根据项目的总体目标、项目范围以及项目进度计划，双方确定有效的项目质量标准。

2. 项目执行过程中，投标人须通过进度报告、例会纪要、里程碑评审等方式持续监测项目质量，发现偏差须在下一工作日内向招标人报告并提出纠正措施；

3. 投标人须保证交付物符合国家相关技术标准、招标人内部信息化管理规。投标人提供的技术方案须符合的标准规范包括但不限于以下：

（1）GB/T 43572-2023 《区块链和分布式记账技术 术语》

（2）GB/T 43575-2023 《区块链和分布式记账技术 系统测试规范》

（3）GB/T 43579-2023 《区块链和分布式记账技术 智能合约生命周期管理》

（4）GB/T 43580-2023 《技术规范区块链和分布式记账技术 存证通用服务指南》

（5）GB/T 43582-2023 《区块链和分布式记账技术 应用程序接口 中间件技术指南》

（6）GB/T 42752-2023 《区块链和分布式记账技术 参考架构》

（7）GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》

（8）《中国南方电网有限责任公司信息化项目建设管理细则》

（9）《南方电网公司数字南网建设技术架构管控工作指引（试行）》

（10）《中国南方电网有限责任公司软硬件平台架构和资源分配指导意见》

(11) 《关于进一步加强公司信息化项目和数据管理工作的通知》

(12) 《中国南方电网有限责任公司网络安全和数字化工作管理规定》

(13) T/GZBIA 001 - 2025 《政务区块链建设规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日

(14) T/GZBIA 002 - 2025 《政务区块链技术安全规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日

(15) T/GZBIA 003 - 2025 《政务区块链跨链数据格式规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日

4. 投标人须在技术方案中逐项说明本方案对上述标准的符合情况，对暂不符合条款须说明原因及后续整改计划。

5. 本项目涉及区块链平台、跨链接口、可信数据交换等核心模块，投标人须采用经过验证的成熟技术方案，既能够保证先进性和成熟性，也可保证系统的适用性。

（三）沟通保证

投标人须识别本项目的全部利益相关方，包括招标人内部各业务部门及外部对接主体；项目实施期间，采用项目例会、周报、专项会议等多种沟通方式，确保信息及时同步；所有沟通结果须形成书面记录归档；涉及外部平台对接的沟通，投标人须同步抄送招标人，不得单独与外部主体达成影响项目范围或技术方向的协议。

（四）知识转移保证

投标人须在项目实施全程安排招标人关键用户参与需求分析、方案评审、测试验收等核心环节，确保投标人团队充分理解系统设计逻辑；项目交付物须包含完整的系统文档、操作手册、运维指南及二次开发规范；项目验收前，投标人须完成对招标人运维团队的技术培训，培训内容须覆盖系统日常运维、故障处理及常规配置调整，培训效果经招标人考核确认。

3.5 项目功能需求与设计要求

3.5.1 业务需求

基于南方电网区块链广州供电局区块链平台已实现与广州政务区块链“穗智链”的跨链对接基础，以及目前广州供电局正在开展的南方能源行业可信数据空间建设任务及需求，本项目需构建覆盖存证、验证、流通、共享全流程的区块链可信数据管理能力。系统须实现跨链互操作机制与跨链数据双向核验能力，并基于“区块链数据要素 X”框架，开发并部署典型业务场景应用。

3.5.2 功能需求

3.5.2.1 跨链互操作能力优化

实现基于区块链的双向可信核验机制，需实现跨链数据传输前的身份认证与授权核查，以及传输过程中的数据完整性校验（如基于哈希值比对或数字签名技术），确保数据在源链与目标链间一致且未被篡改。

应支持跨链操作的事务一致性保证。若跨链操作部分失败，需具备事务补偿或回滚机制，确保数据的最终一致性，防止数据在不同链上状态不一致。

3.5.2.2 区块链可信数据交换平台

为所有需要流通的电力数据生成包含时间戳、数据哈希、数字签名等信息的唯一存证凭据，并记录于区块链上，确保数据不可篡改、可追溯，实现数据可信存证。

平台需支持基于角色或属性的访问控制策略，约定数据访问权限的模式，确保数据仅在授权范围内被使用，防止数据超范围扩散。

平台应记录数据从申请、授权、传输到使用的全过程日志并上链存证，提供可视化的查询审计界面，满足合规性审查与监管要求，实现数据流通全链路追溯。

3.5.2.3 “电政通”功能模块

开发“电政通”功能模块及链码服务组件，将“区块链+可信认证”“电子证照”“电子签章”等能力封装为标准 API，为上层应用提供统一的标准服务接口；同时，将“区块链+数据确权”“跨链验证”“可信交换”等核心能力封装为可复用、可灵活调用的标准 API 或功能模块，以快速支撑多

样化的“电务+政务”一网通办的融合应用场景开发。开发业务接入模块，实现各类电力业务系统对“电政通”服务组件的便捷接入。配套可视化服务能力，提升可观测性及管理效率。投标方需编制统一系统对接指引，用于规范应用场景接入到电政通模块、外部业务系统与电政通模块跨链对接的流程及接口标准，为各接入方提供清晰、可操作的技术指导。

3.5.2.4 区块链+电力惠民服务

依托跨链互操作与区块链可信数据交换平台，深化“数据要素×惠民服务”创新应用。通过构建民政低保人员权威数据的链上流转与核验机制，打造安全、合规的“区块链+低保优惠”专属服务能力，为各项惠民政策（如电费减免等）的精准落地与即时兑现提供坚实、可信的数据底座支撑。

3.5.3 应用功能

本项目升级区块链平台广州边缘节点，建设区块链可信数据交换平台，提供“电政通”跨链数据校核能力，涉及4项一级应用功能、15项二级应用功能。



3.5.3.1 升级区块链跨链互操作能力

3.5.3.1.1 跨链中继服务

对接广州政务区块链“穗智链”，通过跨链中继服务实现政务数据的跨链查询验证与存证能力。

3.5.3.1.2 区块链平台适配

通过封装与适配现有区块链平台 SDK，在兼容旧链业务系统的基础上，使系统具备接入广州政务区块链“穗智链”进行跨链查询、存证及验证的综合中继服务能力。

3.5.3.2 区块链+可信数据交换平台

基于区块链技术构建与广州政务区块链“穗智链”进行可信数据交互的跨链数据交换中枢。它负责向广州政务区块链“穗智链”发起验证请求，并将政务链上返回的验证结果同步回业务系统，从而在业务办理过程中实现政务权威数据的实时核验与链上留痕。

3.5.3.2.1 数据调用方管理

提供完善的数据调用方管理机制，支持对调用方身份信息的全生命周期管理，并具备灵活的 API 访问凭证下发、安全重置能力。

3.5.3.2.2 数据登记

提供业务数据的登记功能。作为跨链交互的“源头字典”，系统通过提取业务数据的元信息与结构定义，为后续的字段映射与跨链流转提供标准依据。

3.5.3.2.3 数据交换

作为跨链数据的安全通道与执行引擎，负责衔接南方电网业务系统与广州政务区块链“穗智链”。系统基于预设的映射规则执行数据的动态转换、路由分发，并对交换行为进行双链存证留痕。

3.5.3.2.4 可信数据核验

为业务系统使用跨链数据提供可信赖的校验支撑。通过将业务方接收到的数据特征与广州政务区块链“穗智链”上的存证记录进行比对，并结合预设的业务规则，确保数据在流转与使用过程中的真实性、完整性及有效性。

3.5.3.2.5 可信数据溯源

基于区块链技术构建全链路数据溯源能力，实现南方电网区块链与广州政务区块链“穗智链”数据交换过程的全程追溯，确保跨链流转全过程的真实性与不可篡改性。

3.5.3.2.6 账本管理

具备账本全生命周期管理能力，支持多维度的账本初始化定义、快速检

索及信息动态维护，并提供可视化的状态管控机制以实现对底层账本访问的实时准入控制。

3.5.3.2.7 配置管理

3.5.3.2.7.1 账本参数配置

支持对账本数据结构的动态定义与参数化配置，允许用户自定义业务字段的名称及数据类型，并提供灵活的参数列表管理与维护机制，以实现对不同业务场景数据模型的精准适配。

3.5.3.2.7.2 账本校验规则配置

建立完善的跨链数据合规校验机制，支持用户自定义账本校验规则及适用场景，并提供规则的全生命周期管理与可视化启停控制，以确保上链数据的准确性与业务逻辑的一致性。

3.5.3.2.7.3 账本校验规则校验字段配置

支持对账本校验规则的底层字段进行动态配置，允许用户灵活定义校验字段的数据格式与关联逻辑，并提供标准化的字段维护机制，以实现对跨链数据质量的精确比对与合规管控。

3.5.3.2.7.4 数据调用方-账本校验规则配置

须支持数据调用方与账本校验规则的灵活绑定，通过提供可视化的规则配置与状态启停管理，实现对 API 接入方调用广州政务区块链“穗智链”核验行为的精细化策略管控。

3.5.3.2.8 数据交换日志管理

提供全量跨链访问日志拦截与审计机制，支持对 API 调用流水进行实时记录、多维检索及统计分析，并具备日志导出能力，以满足系统运维审计需求。

3.5.3.3 “电政通”功能模块

3.5.3.3.1 链码服务组件

链码服务组件作为衔接广州政务区块链“穗智链”与业务应用系统的核心纽带，负责将广州政务区块链“穗智链”底层的“区块链+可信认证”、“电子证照”、“电子签章”等核心能力进行高度封装。通过屏蔽异构区块链底层协议的复杂性，对外提供标准化的 API 接口，支撑业务系统合规、高效地

使用政务侧可信服务。

3.5.3.3.3 业务接入模块

为各类业务场景提供统一的接入管理能力。支持用户创建业务接入场景，配置场景基本信息、归属部门等为业务系统快速对接政务区块链提供场景化的配置支撑。

3.5.3.3.4 数据可视化

须提供全景式数据可视化大屏，通过集成化看板实时监测调用方接入、账本活跃度及 API 核验统计等核心运营指标，实现对跨链交换平台全局业务状态的直观监控与数据洞察。

3.5.3.4 “区块链电力数据要素 X” 场景应用

支持“区块链+电力惠民”典型场景应用，利用跨链技术合规调取并验证政务端低保等权威数据，通过建立即时可信的核验机制，实现电费补贴、绿色通道等惠民政策的精准下达与自动化核验。

3.6 技术要求

3.6.1 技术架构要求

3.6.1.1 技术架构

本项目涉及系统遵循《南网云总体架构和技术要求》《南网云微服务开发设计技术要求》等云化微服务化的技术要求，数据底座符合底座式云化数据中心的数据管控技术要求。

平台总体架构应包括基础设施层、区块链支撑服务层、区块链数据管理层、区块链应用层等核心层次，以及贯穿各层的区块链运行监控功能。

本项目对原广州供电局区块链平台进行升级改造，重点开发部署区块链数据管理系统和区块链运行安全监控系统，提供该区块平台对可信数据存在和流通的技术支撑能力。

3.6.1.2 技术路线

本项目数据处理架构须依托招标人“底座式”数据中心的数据存储能力和数据处理能力，完成项目数据的接入、模型建立及数据处理计算，不得另行建设独立数据处理体系。项目应用架构须遵循招标人微服务架构规范进行

应用开发，并基于招标人“南网云”进行部署运行，构建灵活、高效的微服务集群，实现服务的高可用、高性能、高扩展。具体如下：

（一）系统架构

系统须采用 B/S 架构，实现前后端分离，前后端通信须采用 HTTP RESTful 接口方式。

（二）前端技术

前端须采用 HTML5、CSS 等主流 Web 技术实现，支持丰富的图形化展示能力，具备良好的浏览器兼容性。

（三）后端技术

后端须采用主流微服务框架实现，微服务间通信支持 HTTP RESTful 或消息队列方式，并具备数据缓存能力。

（四）数据存储

数据存储须采用自主可控数据库，优先选用达梦数据库等国产数据库产品，满足数据同步、数据存储及数据处理需求。

3.6.1.3 技术分类

本次建设涉及的技术分类情况，如下表所示：

技术域	一级技术分类	二级技术分类
技术平台	区块链平台	软件工具包
技术平台	区块链平台	区块链服务层
技术平台	区块链平台	区块链服务功能组件

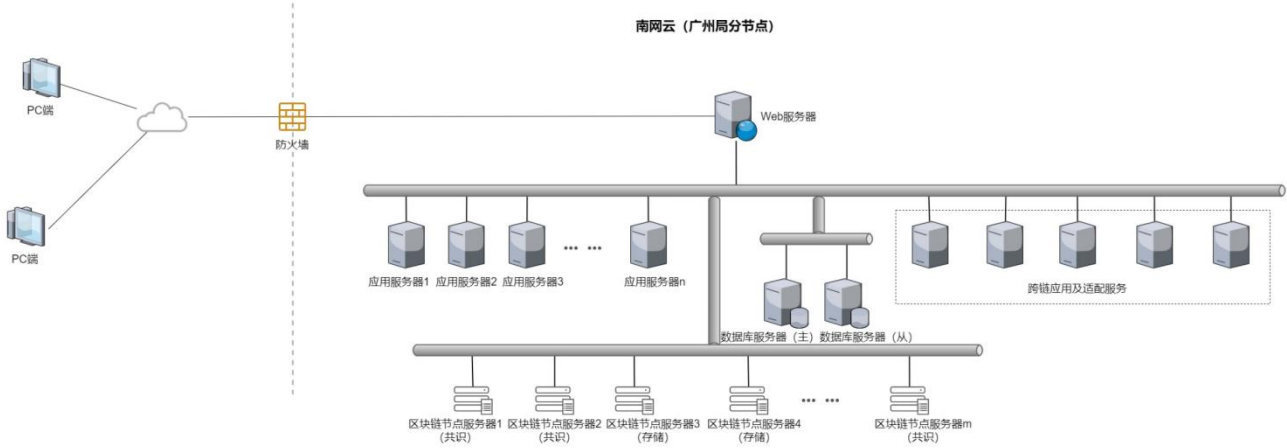
3.6.1.4 技术组件

技术域	一级技术分类	二级技术分类	技术组件
技术平台	区块链平台	软件工具包	可信数据交换
技术平台	区块链平台	区块链服务层	电政通链码模块
技术平台	区块链平台	区块链服务功能组件	区块链数据要求 x 场景应用

3.6.2 部署方式与软硬件要求

3.6.2.1 部署方式

系统采用南网云（广州局）分节点集中部署，统一通过综合数据网络接入并访问应用，系统用户包括广州局本部及下属各单位。项目涉及的所有广东电网的数据接入数据中心广东分节点，确保以公司数据中心作为基础数据底座的建设模式，系统部署结构如下图所示：



3.6.2.2 软硬件资源需求

本项目所需硬件资源由招标人通过云资源或虚拟化资源方式统一提供，硬件资源投资不在本项目列支，投标人报价中不得包含硬件采购费用。基础软硬件须满足自主可控要求。

3.7 自主可控要求

1、优先使用《南网云平台技术白皮书》所发布的服务与组件，采用南网云平台的中间件、数据库组件、计算、存储资源等技术或开源技术保证自主可控。

2、项目建设阶段，要求围绕《南方电网公司全栈自主可控技术路线目录（2024）》开展产品差异分析及设计，设计方案参考《南方电网公司系统自主可控适配典型设计参考（2024版）》，且后续根据上述文件同步更新迭代。

3、本项目涉及的所有应用和软硬件产品必须符合自主可控要求，且本项目涉及的所有应用能够适配未来自主可控环境潜在变化需求，目前南方电网公司 CPU、操作系统、数据库、中间件、计算机终端、浏览器、开源软件及关键组件等自主可控选型适配设计情况包括但不限于：

1) CPU：计算机终端 CPU 要求兼容自主可控 CPU（ARM、MIPS、X86、ALPHA

等）架构，根据项目业务需求选择自主可控 CPU（如龙芯、兆芯、飞腾、鲲鹏、申威、海光等）。服务器 CPU 要求兼容自主可控 CPU（ARM、MIPS、X86、ALPHA 等）架构，选型要求确保系统的稳定性、可靠性以及满足特定的性能需求，包括不限于飞腾、鲲鹏、海光等产品。

2）操作系统：兼容国内主流桌面、服务器自主可控操作系统（如统信 UOS、银河麒麟、麒麟信安等）。

3）数据库：要求兼容国内主流自主可控数据库（包括不限于达梦、金仓等）。

4）中间件：兼容国内主流自主可控中间件（如：中创等）。

5）浏览器：兼容统信浏览器、麒麟奇安信浏览器、360 安全浏览器、搜狗浏览器、红芯浏览器等自主可控浏览器，应用系统可与支持国密算法的国产浏览器加密通信。

6）开源软件及关键组件：要求开源软件及关键组件自主可控，选型过程中评估这些组件与现有系统的兼容性和可替代性。

3.8 技术标准与规范引用

应符合区块链已发布的有关标准。

（1）GB/T 43572-2023 《区块链和分布式记账技术 术语》

（2）GB/T 43575-2023 《区块链和分布式记账技术 系统测试规范》

（3）GB/T 43579-2023 《区块链和分布式记账技术 智能合约生命周期管理》

（4）GB/T 43580-2023 《技术规范区块链和分布式记账技术 存证通用服务指南》

（5）GB/T 43582-2023 《区块链和分布式记账技术 应用程序接口 中间件技术指南》

（6）GB/T 42752-2023 《区块链和分布式记账技术 参考架构》

（7）GB/T 22239-2019 《信息安全技术网络安全等级保护基本要求》

（8）《中国南方电网有限责任公司信息化项目建设管理细则》

（9）《南方电网公司数字南网建设技术架构管控工作指引（试行）》

（10）《中国南方电网有限责任公司软硬件平台架构和资源分配指导

意见》

(11) 《关于进一步加强公司信息化项目和数据管理工作的通知》

(12) 《中国南方电网有限责任公司网络安全和数字化工作管理规定》

(13) T/GZBIA 001 - 2025 《政务区块链建设规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日

(14) T/GZBIA 002 - 2025 《政务区块链技术安全规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日

(15) T/GZBIA 003 - 2025 《政务区块链跨链数据格式规范》，发布单位：广州市区块链产业协会，发布日期：2025 年 12 月 10 日，实施日期：2026 年 1 月 1 日

3.9 安全技术方案

3.9.1 总体安全防护要求

1、按照“同步规划、同步建设、同步投运”原则加强本系统的网络安全防护，确保不发生重大及以上信息安全事件是本系统建设与运行的网络安全防护底线。

2、需要根据《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019) 及云计算、移动互联、物联网和工业控制系统等拓展要求，进行本系统的建设、定级、防护、测评及备案，确保关键信息基础设施安全。

3、需要根据《信息安全技术 信息系统密码应用基本要求》(GB/T 39786-2021) 实现国产密码应用，并对接公司统一密码服务平台以实现密码等服务的统一管控和认证。

4、需要遵循国家发改委《电力监控系统安全防护规定》（2024 年第 27 号令）以及国家能源局《电力监控系统安全防护总体方案等安全防护方案和评估规范》（国能安全〔2015〕36 号）等要求，贯彻落实“安全分区、网络专用、横向隔离、纵向认证”十六字方针。

5、需要满足《中国南方电网电力监控系统安全防护技术规范》《南方电网

公司网络安全合规库（2022 年修订版）》《南方电网公司管制类业务网络安全设计导则（2023 年版）》《南方电网公司 IT 主流设备安全基线技术规范》《南方电网公司涉密事项界定范围表》（南方电网办〔2016〕13 号）、《南方电网公司数据共享开放指导意见（试行版）》（信息〔2017〕51 号）等相关要求。

6、需要按照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中国南方电网有限责任公司数据安全管理办法》（Q/CSG2223007-2024）、《南方电网数据安全总体要求技术规范》（Q/CSG1210049-2020）等法律法规相关要求，落实数据安全相关要求。

7、通过数字身份与访问控制中心，实现本系统统一账号、统一认证、统一权限控制、统一审计管理。

8、通过云盾平台，进行本系统的集中监控以及安全态势感知，实现集监测、预警、防护、检测、响应和恢复的动态网络安全管控。

3.9.2 安全保护等级

根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）以及《南方电网管理信息系统安全等级保护标准》要求，本系统的安全等级保护定为二级。并需要按照中华人民共和国国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）进行系统的安全防护。

系统建设完成后按照国家及南网的要求开展系统入网安评及信息系统安全等级测评及备案工作。

3.9.3 物理和环境安全

本信息系统需部署在南方电网公司专业机房内。专业机房需符合国家以及南方电网公司信息机房建设技术规范以及运营相关要求。具备防震、防风、防雨、防雷、防火、防盗等保护措施。机房温、湿度的变化在本系统设备运行所允许的范围之内。

通过符合国产密码要求的电子门禁系统确保机房出入控制；通过符合国产密码要求的视频监控系统实现视频监控。

3.9.4 网络和通信安全

为保证网络层的安全性，需要合理设计网络拓扑结构，并实施网络边界控制措施。

3.9.4.1 网络拓扑结构

网络结构安全保证网络设备的业务处理能力具备冗余空间和链路负载均衡能力，满足业务高峰期需要。

根据本系统的安全属性，其部署在信息内网。并按照“三级（及以上）系统独立成域、二级（及以下）系统集成成域”的原则，通过虚拟化网络技术或者 SDN 技术实现本系统单独设域，与其他系统实现逻辑隔离，在不同网段之间进行路由控制，建立安全的访问路径，实行针对性、差异化防护。

涉及 internet 的应用，需部署在信息外网区，使用统一集中的互联网出口，并通过信息安全交换平台实现强逻辑隔离。

要求采用冗余技术设计网络拓扑结构，确保路由冗余。

网络优先级配置：根据本系统的重要性设置带宽分配级别，保证在网络发生拥堵的时候优先本系统服务连续性。

网络设备冗余配置，避免存在网络单点故障，确保网络设备高可靠性。

3.9.4.2 网络通信安全

数据通信中要采用校验技术或密码技术保证通信过程中数据的完整性以及保密性。

3.9.4.3 网络边界防护

通过 ACL 技术或防火墙技术，在网络边界或区域之间根据访问控制策略设置访问控制规则，对本系统域实现端口级访问控制，默认情况下除允许通信外受控接口拒绝所有通信；应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。并对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出，保证信息及网络资源不被非法使用和访问。

通过入侵监测技术，在网络边界处监视如端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等攻击行为，并给警告警以及响应和处理。

在网络边界及核心业务网段处对恶意代码进行检测和清除；及时实现恶意代码库升级和检测系统更新。

通过网络安全扫描工具，利用优化系统配置和打补丁等各种方式最大可能地

弥补最新的安全漏洞和消除安全隐患。

3.9.4.4 网络安全审计

通过信息安全运行预警系统，实现对网络设备、安全设备运行状况、网络流量、用户行为等进行日志信息实时采集、集中监控及实时预警。审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

3.9.4.5 网络安全加固

- 1、对登录网络设备的用户进行身份鉴别。
- 2、禁止采用默认的管理员账号和密码。
- 3、对网络设备管理员登录的地址进行限制。
- 4、通过支持国密算法的 U-key 认证方式登录，key 证书具有唯一性。
- 5、网络设备账号满足密码复杂度设置，并定期进行更新，存储为加密存储方式。
- 6、具有登录失败处理功能，登录 5 次失败后，采取结束会话的措施。
- 7、采取 SSH 加密协议远程管理网络设备。
- 8、已通过服务器区防火墙进行限制，只对系统的特定端口进行开放。

3.9.5 设备和计算安全

3.9.5.1 硬件安全

采用服务器设备具备冗余配置（包括双机热备等）；具备不间断电源保障，具备服务器运行状态监控，确保本系统处理性能要求。

对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；当进行远程管理时，应采取加密措施。

3.9.5.2 操作系统安全

操作系统原则上采用自主可控系统，加强操作系统账号管理、认证授权、安全日志等功能，实现从身份鉴别，访问控制，安全审计入侵防范，恶意代码规范，资源控制几个方面进行主机安全基线加固。

3.9.5.3 中间件安全

从身份鉴别，访问控制，安全审计，通信完整性，通信保密性，软件容错，

资源控制几个方面进行中间件安全基线加固。

3.9.5.4 接口安全

1、认证与授权:实现强认证机制(如 OAuth, JWT),并对访问 API 的用户或服务进行细粒度的授权。

2、输入验证:对所有外部输入进行严格验证,防止 SQL 注入、XSS 等攻击。

3、输出编码:在返回响应之前对输出数据进行适当的编码,防止注入攻击。

4、限流与防滥用:通过速率限制和访问控制防止接口被滥用。

5、日志记录:详细记录所有接口调用,以便于审计和异常检测。

6、加密传输:使用 TLS/SSL 等协议加密敏感信息的传输,保护数据不被截取。

7、安全性测试:定期进行安全性测试,包括但不限于渗透测试和安全扫描。

3.9.5.5 组件安全

1、组件选择:选择信誉良好且维护活跃的开源或商业组件。

2、安全配置:按照最佳实践配置所有使用的组件,避免使用默认设置。

3、补丁管理:及时应用组件的安全更新和补丁。

4、隔离原则:尽可能将不同功能的组件隔离开,限制它们之间的交互,减少攻击面。

5、最小权限原则:为每个组件分配最小必要的权限,以降低潜在风险。

3.9.5.6 数据库安全

禁止采用默认的管理员账号和密码,避免非法用户进入网络后通过直接调用监控末端设备查看相关信息。

3.9.6 应用和数据安全

3.9.6.1 数据安全

系统数据不涉及商业秘密,涉及个人信息,采用身份认证、权限控制、加密存储、加密传输、数据防泄密等技术,加强本系统数据机密性及安全性防护:

1、通过对数据库表设置完整性约束,如 Check、NOTNULL、Unique、Primary、Foreignkey 来保证数据的完整性。

2、宜使用国产密码技术对本系统数据库表访问权限进行控制。

3、宜采用国产密码技术对本系统的重要数据进行加密存储,防止数据库被黑客攻击导致系统机密泄漏。

- 4、宜使用国产密码技术保证本系统重要数据传输过程中的机密性及完整性。
- 5、仅采集和保存业务必需的用户个人信息；禁止未授权访问、使用用户个人信息。
- 6、宜通过数据防泄密网关，减少敏感数据泄密。
- 7、采用数据本地备份或者数据灾备技术，确保本系统核心数据安全，确保在某个存储设备故障或灾害发生时，数据不会丢失。
- 8、存储设备报废前按照规定宜通过消磁粉碎一体机进行信息彻底清除，确保数据不能被恢复、还原。
- 9、本系统日志信息宜保持 6 个月以上。并采用国产密码技术实现本系统日志信息完整性保护。
- 10、宜采用国产密码技术实现本系统的加载和卸载安全控制。
- 11、实现数据库访问审计。

3.9.6.1.1 数据分类分级设计

遵循数据安全合规保护要求及数据安全成熟度模型，结合公司敏感数据分类分级规范，在系统/平台设计之初对业务系统的数据分级分类，为后续数据保护策略提供基础，建立起完善数据全生命周期的安全保障措施，确保数据采集、传输、存储、使用、共享、销毁全过程中的安全。（数据分级分类过程及标准参考《南方电网数据安全总体要求技术规范》）

3.9.6.1.2 数据安全防护技术设计

3.9.6.1.2.1 数据传输机密性及完整性设计

针对涉及到客户重要信息加密等具有传输机密要求场景，通过调用统一密码服务对重要数据在传输过程中进行加密和签名，使用 SM3 国密签名算法、SM2 非对称算法、SM4 对称算法。保障数据传输过程的机密性和完整性。

3.9.6.1.2.2 数据存储机密性及完整性设计

针对涉及到客户重要信息加密等具有存储机密要求场景，调用统一密码服务在数据存储时加密入库，使用 SM4 国密对称算法、国密签名算法保障数据存储的机密性和完整性。

3.9.6.1.2.3 数据共享脱敏安全设计

针对涉及对外部共享数据时，需要脱敏的数据通过数据脱敏服务接口发送给

脱敏，对于数据中的敏感数据进行脱敏处理（遮蔽/变形/伪装），达到数据的安全应用和防泄露效果。

3.9.6.2 应用安全

1、采取三权分立，本系统应具备完善的权限管理，贯穿全系统的分级授权和界面信息操作控制，完整的应用程序日志记录和审计机制。

2、提供访问控制功能，通过角色划分实现各层各级人员对于功能页面的访问控制；依据安全策略控制用户对文件、数据库表等客体的访问；访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；授权主体配置访问控制策略，并严格限制默认账户的访问权限。

3、实现对登录用户的统一身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证本系统用户身份的真实性。

4、启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

1) 用户身份鉴别信息应不易被冒用，口令复杂度应满足要求并定期更换。应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；用户在第一次登录系统时修改分发的初始口令，口令长度不得小于 8 位，且为字母、数字或特殊字符的混合组合，用户名和口令禁止相同；应用软件不得明文存储口令数据；

2) 提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

3) 授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

4) 及时删除或停用多余的、过期的账号，避免共享账号。

5、采用基于国产密码的数据验签技术保证通信过程中数据的完整性；

6、通过基于国产密码的加解密技术，实现对重要数据的传输安全防护。

7、通过基于国产密码的加解密技术实现数据有效性检验功能

8、加强数据有效性检查，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

9、关闭不需要的端口及服务。

10、通过负载均衡技术，确保在突发数据流的情况下，本系统依然可以提供适当的服务能力。

11、当通信双方中的一方在一段时间内未作任何响应，另一方自动结束会话；对系统的最大并发会话连接数进行限制；对单个账号的多重并发会话进行限制。

12、通过防病毒系统，实现统一控制台对应用系统病毒防范，包括统一的分发、维护、更新和报警等。

13、通过对用户的登录、退出、增加用户、修改用户权限等进行应用审计。

14、通过云盾平台，实现对本系统的运行状态、用户体验等的实时监控与预警。

15、要求通过支持国产密码的堡垒机等技术，实现对本系统运维的统一管控，避免对网络和服务器资源的直接访问，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为，减少恶意攻击，拦截非法访问，并实现运维操作行为审计。

3.9.6.3 移动应用安全管控

不涉及。

3.9.6.4 集成安全管控

1、涉及接入其他系统时，根据接入要求完成接入，同时确保数据交互通道安全。

2、业务系统接入本系统时，要制定详细的接入文档，同时接口添加权限校验，确保能拦截非法接入，数据传输要使用安全传输协议。

3.9.6.5 密码安全

项目对接公司统一密码服务平台以实现密码等服务的统一管控和认证。

3.9.7 终端安全设计

不涉及。

3.9.8 安全管理

3.9.8.1 安全管理机构与人员

设立专职信息安全部门与岗责分明的安全管理员，并严格落实人员背景审查与离岗权限即时收回制度。

3.9.8.2 安全策略和管理制度

严格遵循南方电网公司网络安全总体方针，实施访问控制策略，杜绝网络资源的非法调用与越权操作，建立合法合规的体系化安全操作规范及常态化人员培训机制。

3.9.8.3 安全建设管理

交付产品应通过出厂安全测试、入网安全测试、源代码审计等，安全测试发现的高中风险全部完成整改, 并完成系统的等保定级。

3.9.8.4 安全运维管理

建立集中的监控预警与快速响应机制，落实定期漏洞扫描与数据灾备演练，并承诺由自身核心团队自主运维。

3. 10 性能要求

支持最大用户数不小于 100 人，最大在线用户数 10 人，支持的最大并发用户数不小于 5 人；页面平均响应时间不超过 3 秒；吞吐量每秒处理请求数不超过 20 请求数/秒;资源可用率满足 CPU 可用率<80%, 内存使用率<85%, 运行满足 7*24 小时。

3. 11 实施工作要求

本项目于下达启动之日分阶段、分步骤开展项目开发与实施工作。整个项目周期计划自项目启动之日起至 2027 年 10 月 31 日，具体以合同约定为准。本项目初步实施进度计划如下表所示：

序号	任务名称	预计工期	任务描述
1	项目启动	合同签订之日	完成合同签订工作。
2	需求分析及设计	2026 年 10 月	完成需求分析及设计（概设和详设等）工作
3	系统开发及部署	2027 年 5 月	完成系统功能开发及部署
4	初步验收	2027 年 6 月	完成系统功能验收等工作
5	试运行	2027 年 9 月	系统试运行
6	竣工验收	2027 年 10 月	完成竣工验收工作

3. 11. 1 上线前

3.11.1.1 项目启动

投标人须按照工作方案的目标及要求，组织编制整体实施方案并通过招标人评审。投标人须协助召开项目启动会，明确项目实施负责人、干系人、目标和计划，并配合编制会议相关材料。

3.11.1.2 系统环境准备

投标人须完成服务器环境搭建准备工作，包括资源申请、策略开通、数据库部署、应用服务部署等。完成区块链节点部署与跨链通道连通性验证。

3.11.1.3 系统初始化

3.11.1.3.1 静态数据准备

投标人须完成静态数据环境分析，包括库表完整性、数据同步工具、相关策略开通、权限情况等。在此基础上编制静态数据准备方案，落实各项准备工作任务和交付物，包括角色、岗位、流程、台账基础和业务配置收集模板。投标人须编制静态数据准备工作作业指导书，内容涵盖系统权限（角色、岗位、流程）配置及业务基础数据配置工作操作指引，并在静态数据准备工作开始前组织开展基础数据维护、人员、角色、岗位、流程配置工作宣贯和配置培训。

3.11.1.3.2 动态数据准备

投标人须完成动态数据环境分析，包括软件安装、环境配置参数、数据库空间、中间件、策略开通等工作。在此基础上编制数据清理方案、数据迁移方案和数据验证方案，并编制对应的数据治理工作指引、迁移工作指引和数据验证工作指引。投标人须在动态数据准备工作开始前组织开展数据治理、迁移、验证工作方案宣贯和迁移培训。

3.11.1.4 集成调试

投标人须完成软件集成调试和硬件集成调试两部分工作。软件集成调试须覆盖应用侧与中台或其他系统间集成所涉及的适配、调试工作，包括测试用例编制、环境准备、数据准备、接口调试、测试报告编制及问题处理。

3.11.1.5 最终用户培训

投标人须编写培训教材，可在软件产品厂商或开发厂商提供的培训课件基础上，结合甲方具体情况进行调整优化，或重新编写。投标人须完成培训

场地落实及必要设备部署调试工作，按计划组织对甲方运维人员及相关业务人员开展培训，并对培训成效进行及时评估，对于多批次培训应依据评估结果持续优化培训过程，提升培训质量。

3.11.1.6 上线切换

3.11.1.6.1 上线切换准备

投标人须完成系统切换测试，包括技术验证和业务验证两部分。技术验证内容包括系统基础配置有效性验证、权限配置有效性验证、系统功能测试、性能测试及安全测试；业务验证内容包括编制业务验证指引和用例、组织业务验证培训及组织开展业务验证。投标人须编制系统上线切换方案、上线应急保障方案、上线演练方案及上线试运行方案。投标人须按照上线切换工作方案和演练方案组织开展上线切换演练。投标人须协助策划并组织召开上线启动会，配合完成会议材料的编写、评审、定稿及会议现场准备工作。

3.11.1.6.2 系统上线切换

投标人须按照切换准备工作方案，配合招标方成立切换工作组，开展系统正式环境切换工作。

3.11.2 试运行

3.11.2.1 小版本发布

试运行期间，投标人须解答与处理一线用户问题，包括操作咨询、权限配置等现场可直接处理的问题，须同时覆盖现场和后台人员。对于系统缺陷、功能改进、功能需求等现场不能直接处理的功能性二线问题，投标人须建立管理跟踪机制并及时反馈处理结果。版本发布须开展发布测评并形成测评报告，按照发布作业管理流程完成申请、审批后，依据作业操作票执行版本发布更新，并按照版本问题更新清单组织开展功能测试验证工作。

3.11.2.2 试运行期限

试运行期间，投标人须对应用服务器及数据服务器进行日常运行监控，并开展服务器平台调优与日常维护工作，同时提供系统使用答疑和问题管理服务。试运行期限 1 个月。

3.11.3 运行维护

3.11.3.1 运维模式

项目通过初验后进入试运行阶段，由招标人系统运维部门系统管理员与投标人人员共同组建混合运维团队，共同承担试运行期间的运维工作。所有运维工作须通过招标人指定南网安全堡垒机执行，运维行为由南网安全堡垒机进行全程记录和审计。

3.11.3.2 运维职责划分

试运行阶段，运维职责以项目建设部门为主、系统运维部门为辅。终验通过并完成系统移交后，运维职责转移至招标人系统运维部门承担，职责分工如下：

招标人系统运维部门主要负责核心业务运维，包括核心设备的日常配置管理、重要应用系统的数据管理及用户权限管理等；投标人人员主要负责系统后台运维，包括 BUG 修复完善、性能优化等工作。

3.11.3.3 运维考核

运维期间，甲方将依据合同约定严格开展质检工作，对不达标的运维工作进行考核。运维费用依据《南方电网公司信息化项目预算编制与计算方法》等标准，通过年度例行信息系统维护等项目统筹考虑。

3.12 测试要求

投标人须对本项目涉及的所有功能模块和系统集成内容开展全面测试，测试须覆盖功能、性能、安全等多个维度，合理设计测试方案和测试用例，选用适当的测试工具，搭建符合要求的测试环境，测试完成后提交真实完整的测试报告，并对测试中发现的问题进行闭环处理。

具体测试工作包括：代码开发完成后组织单元测试和集成测试；系统测试版本发布后，配合开展第三方性能测试和安全测试，并组织功能测试；上线前须完成联调测试，确保本项目与招标人内部业务系统及外部对接平台之间的集成功能满足要求，联调测试须覆盖本项目所涉及的全部内容，并遵从招标人统一协调安排。

3.13 项目转分包要求

1. 投标人不得将本合同项目转包给第三方。
2. 原则上不允许投标人将本合同项目分包给第三方，如确有需要，必须经招标人许可，投标人方可将本合同项目部分内容分包给第三方，且分包必须符合

以下条件：

- (1) 合同项目的主体部分不允许分包给第三方；
- (2) 合同项目分包给第三方的比例不能超过或等于合同总额的 30%；
- (3) 合同项目不允许分包给不符合相关资质要求的第三方；
- (4) 合同项目只允许一次性分包。

四、项目实施

技术联络组

由招标人、投标人分别指派人员组成技术联络工作组，该组负责在系统开发、试点实施过程中组织召开必要的技术联络会议。

招标人验收组

招标人验收组织部门须成立验收委员会，验收委员会由业务部门和数字化部门专家组成，必要时可以邀请项目建设单位以外的代表及专家参加。

招标人验收组负责组织对系统进行验收。同时，验收组指导项目测试、技术资料小组进行项目资料的收集、整理和编印。

4.1 时间进度安排

根据数字化部工作安排，项目工期自合同生效之日起至 2027 年 10 月 31 日。

4.2 技术联络

投标人须在项目实施期间与招标人建立项目联络会制度，定期组织召开技术联络会，协调解决项目推进过程中的相关事宜，审查阶段性成果及质量，跟进项目进度。联络会须覆盖项目启动、阶段成果确认、技术文件审查、培训计划确定、验收细则确认等关键节点，涉及外部平台对接的协调事项须同步纳入联络会议程。投标人负责组织联络会并提供必要的会议材料，会议结论须形成书面纪要，经双方确认后执行。

4.3 验收

本项目验收严格按中国南方电网公司信息化项目验收相关规定进行。

投标人应在分别具备项目初验（功能验收）、项目终验（竣工验收）条件后向招标人提出验收申请，招标人应在收到投标人验收申请后及时答复投标人，并在验收申请审批通过后的十个工作日内组织召开验收会。

项目初验

开发项目满足以下条件并提交相关成果通过审查时，投标人可申请项目初验：

1. 项目已完成开发工作，具备试运行条件；
2. 系统已通过功能、性能、安全测试；
3. 项目已遵照培训计划完成相关培训。
4. 如果项目存在监理方，须获得监理质量评估报告；

招标人审批投标人提交的项目初验申请，当确定项目满足验收条件后组织验收会议。招标人业务部门参与验收。

项目终验

项目满足以下条件并提交相关成果通过审查，投标人可申请实施终验：

1. 系统试运行一个月；
2. 用户手册已通过审核；
3. 运维手册已通过审核；
4. 系统运行报告已通过审核；
5. 如项目存在监理方时，获得监理质量评估报告。

招标人审批投标人提交的项目终验申请，当确定项目满足验收条件后组织验收会议。招标人业务部门参与验收。

4.4 培训

投标人须向招标人提供完整可行的培训方案，并严格按照培训计划完成相关培训，实现本项目成果和知识由投标人向招标人的有效转移。培训须包括以下两类：

系统管理维护人员培训：针对招标人系统运维人员开展技术培训，内容须覆盖系统日常维护、常规故障处理及系统管理工具使用，使其具备独立完成系统日常运维工作的能力；

业务操作人员培训：针对与本项目业务场景直接相关的操作人员开展应用培训，使其熟悉系统功能并熟练掌握对应业务场景的系统操作。

投标人须在验收前完成全部培训并提交培训记录，培训效果经招标人确

认。

4.5 项目交付项

投标人应在合同规定时间内，按照广州供电局 PMO 管理规范要求及审计要求，向招标人提供相应交付物及服务报告，包括但不限于：（可选填）

（1）系统初验交付物，包括：

1. 实施工作方案；
2. 需求分析规格说明书；
3. 系统概要设计说明书；
4. 系统数据接口方案；
5. 系统详细设计说明书；
6. 系统数据设计说明书；
7. 系统测试用例；
8. 系统测试报告；
9. 第三方性能、功能测试报告；
10. 入网安全评测报告；
11. 用户使用手册；
12. 系统管理员手册；
13. 运维手册；
14. 安装配置手册；
15. 系统投运方案；
16. 系统启停作业指导书（含系统运行正常检验标准）；
17. 系统定期维护作业指导书；
18. 软硬件配置及关联关系表、资产台帐；
19. 培训计划、培训记录；

（2）系统终验交付物，包括：

- 1、初步验收遗留问题整改报告；
- 2、系统运行报告；
- 3、系统运行报告审核报告；
- 4、系统现场处置方案；

5、系统实用化工作方案、系统实用化评价细则；

6、用户问题列表；

7、故障列表；

8、培训计划、培训记录；

4.6 知识产权要求

投标人在本项目中专门开发或定制的工作成果，其知识产权归招标人所有，包括但不限于为本项目产生的文档、报告、程序、脚本、工具、软件及相关文件和文档的版权等。

投标人在本项目实施过程中使用的自有技术、已有组件、底层框架或第三方授权组件，其知识产权归原权利人所有，但投标人须确保上述内容的使用已获得合法授权，不侵犯任何第三方知识产权，并在技术方案中明确说明自有或第三方组件的使用情况及授权来源。

本项目产生的软件著作权、发明专利申报材料，专利申请权及获得的专利权归招标人所有，投标人须配合招标人完成专利申请相关工作。

未经招标人书面许可，投标人及其任何人员均不得行使本项目工作成果的任何知识产权。

招标人需就项目成果申请专利或者著作权备案的，投标人应予以协助。招标人需将相关成果形成论文或申请专利或进行软件著作权登记的，投标人应予以协助。配合提交至少 2 项发明专利申报材料。

五、服务方案

本项目涉及区块链平台升级、跨链互通对接及区块链可信数据交换平台建设，技术架构复杂，外部协调工作量大，投标人应提供完善的、基于本项目实际业务场景的技术服务方案。

评审时将对各投标人服务方案的科学性、合理性与完整性进行横向比较，综合评价内容包括：技术方案的针对性与可行性、项目计划与进度安排的合理性、质量管理措施的具体性、外部协调工作的应对策略，以及服务全周期的保障能力。

六、服务团队及服务能力

（一）团队规模

投标人须配置不少于 5 人的项目实施团队，团队成员须覆盖项目管理、区块链架构、软件开发、测试等关键角色，各角色须有明确的人员配置及职责分工。

（二）团队能力要求

团队成员资质要求：计算机技术与软件专业技术资格中级或以上证书不少于 2 人。

团队须具备区块链平台开发及跨链对接的实际项目经验，核心成员能够提供参与区块链相关项目的证明材料。

团队具备完整的区块链项目文档交付能力，包括但不限于技术架构设计文档、接口规范说明、部署运维手册及用户操作指南等。

团队成员具备跨机构数据流通项目的协调对接经验，能够提供与外部机构进行技术对接及业务沟通的实际案例说明。

（三）项目负责人要求

1. 具备 3 年以上信息化项目管理经验，其中至少主导过 2 个以上区块链相关项目的全周期实施，能提供相应项目合同或验收证明；

2. 具有区块链跨链互通、多链协同或可信数据交换相关项目经验者优先，须提供对应项目案例说明；

3. 充分理解本项目的背景、目标、建设范围及重难点，能够准确识别跨链对接、外部平台接入等核心风险点，并在答辩或技术方案中提出针对性解决方案；

4. 具备跨机构协调能力，有涉及外部主体对接或多方协同项目经验者优先；

5. 具备向非技术背景管理人员清晰传递项目进展与技术风险的能力；

服务团队及服务能力具体要求详见《服务团队优异性表》、《一般服务团队条款/参数应答表》。

七、进度计划及保证措施

投标人须根据本项目合同工期制定科学可行的进度计划，明确可研阶段、需规概设阶段、详细设计阶段、开发测试阶段、初步验收、竣工验收各阶段的里程碑节点和交付物，经甲方确认后严格执行，并定期向甲方汇报进度情

况，对偏差及时提出调整方案。

八、服务质量保障措施

具有区块链相关项目售后服务经验的投标人优先。评审时将对以下内容进行综合评判：售后服务体系的完善性、项目团队开展售后服务的组织形式、承诺的售后服务响应方式及响应时间、技术服务支持的针对性与全面性。

九、服务承诺

投标人须承诺在本项目合同履行期间无重大质量事故记录，且在提交投标文件时不存在因本项目相关业务引发的未结法律诉讼。投标人须对本项目的服务质量、响应时效及交付成果作出明确承诺，并对承诺内容承担相应责任。

十、售后服务和技术支持

项目通过终验后投标人提供为期一年的质量保证期。投标人对本项目做出如下的服务承诺：

10.1 质保期服务内容

在质保期内，投标人应负责本项目所开发信息系统的质保服务，确保系统安全、稳定、正常地运行，投标人根据要求提供系统支持服务、系统故障处理、定期巡检等服务，并在约定或招标人要求的时限内响应并排除招标人报告的故障、缺陷。具体质保期服务内容如下：

系统支持服务

本项目的保质期为系统建设竣工验收合格之日起一年，保质期内投标人需免费为项目提供包含以下系统支持服务：

➤ 电话热线服务

配备有经验的售后工程师接听客服电话，及时响应招标人提出的系统问题。

要求响应时间范围为 7×24 小时。响应速度为 10 分钟以内。

➤ 远程支持

对于客服电话解答不了的问题，由售后工程师通过远程网络连线至主机进行远程支持。

要求响应时间范围为：7×24 小时。响应速度 30 分钟以内。

➤ 现场服务

对出现不能远程解决的问题，或在系统的运行环境不完全成熟的条件下，需要提供售后工程师的上门服务，现场解决问题。

要求响应时间范围为：7×24 小时，响应速度 30 分钟以内，120 分钟到达现场。

系统故障处理

故障应急服务：一般故障包括系统性能严重下降及系统功能异常，投标人负责向招标人提供 7×24 小时专人应急服务热线，投标人接到招标人应急报障后，10 分钟内通过电话进行应急响应支持，若 30 分钟仍无法排除故障，且发生的故障或异常暂不影响业务正常运行时，应在 2 小时内赶到现场提供技术支持，投标人工程师到达招标人现场后，立即进行系统补丁、更换硬件部件等措施。故障排除 7 个工作日内，提供《故障应急处理报告》及故障彻底消除解决方案，协助招标人维护人员实施相关的系统升级、参数设置调整。

投标人应招标人要求现场协助招标人维护人员实施系统升级、补丁安装、参数设置调整、应用升级和调整。

在年终结算及法定节假日，投标人提前向招标人提供值班工程师名单、当值地点及联系电话。保障实时响应招标人的故障呼叫，需要时及时赶到现场。

定期巡检服务

投标人每三个月一次派经验丰富的工程师到招标人现场对招标人的质保服务对象进行针对性巡检，检查内容包括：

1、硬件巡检

对负载均衡、服务器、网络设备等的运行情况进行巡检。

2、应用系统巡检

对应用系统日志分析、性能、接口服务联通情况进行巡检。

3、系统分析诊断

根据巡视服务情况，从服务器、数据库、中间件、操作系统、应用系统几个维度进行系统性诊断，分析负载、资源分配等指标，评估数据增长带来

的压力，及时发觉潜在隐患，给出整体诊断报告。

4、其他内容

完成巡检后 3 个工作日内向招标人提交《巡检服务报告》。

10.2 技术服务承诺

在质保期结束后，为满足招标人业务发展需要，若招标人提出软件升级或变更要求，投标人均应提供技术服务，服务费用另行协商。

十一、响应要求及服务评价标准

11.1 事件响应服务要求

事件响应流程必须满足广东电网有限责任公司广州供电局 IT 服务管理规范流程要求，具体事件响应要求如下：

编号	分类	事件	响应时间	到达现场时间
1	紧急	系统所有功能模块无法提供服务，导致系统瘫痪。	10 分钟	120 分钟
		等级 1 的系统出现对外访问故障。		
		等级 1 的系统严重问题消缺。		
2	高	使用频率非常高的功能或者页面发生严重错误，相关业务无法流转到下一个环节，导致系统无法继续使用，并且没有其它功能或者方法可以弥补所造成的影响。	10 分钟	2 小时
		等级 2 的系统严重问题消缺。		
3	中	使用频率较高的模块或者页面发生严重错误，对系统	10 分钟	2 小时

编号	分类	事件	响应时间	到达现场时间
		的正常使用造成严重影响，但是经过处理可以恢复继续使用，或者有其它功能或方法暂时弥补问题造成的影响。3 个或以上用户反复报相同故障。		
4	低	使用不是很频繁的功能或者页面发生细小差错或用户界面显示格式等，通常不影响系统的正常使用。	20 分钟	按实际需要和广州局管理规定要求
5	一般	一般问题消缺	30 分钟	按实际需要和广州局管理规定要求

注：

1、系统等级划分说明

系统等级 1：对于 7*24 提供对外服务的系统，例如营销、营配，协同办公、安全生产等系统，物理环境及基础平台。

系统等级 2：对于提供内部用户服务的系统，例如资产、GIS、OA 等系统

系统等级 3：对于提供内部用户服务的小系统，例如财务、制度管理、党建、计生等系统

系统等级 4：其他系统。

响应时间：投标人服务人员确保电话畅通，接收到报障通知并确认的时间。

到场时间：从响应时间开始算起；

解决时间：从响应时间开始算起；

11.2 服务水平评价

甲方按照以下方式，对乙方提供的服务进行考核评价，起始总分为 80 分。

一级指标	二级指标	序号	评价内容	取证依据	加分及扣分标准
人员配置	人员数量	1.1	按照本协议要求配备足够的工作人员。若不满足约定的人员梳理，按扣分标准进行扣分。	依据本协议要求，参考日常工作签到表。	-2 分/人
	人员素质	1.2	团队安全服务人员（个人）累计发现高危风险数（人工渗透测试漏洞，人工基线核查）超过 25 个的		5 分/人
	人员素质	1.3	团队安全服务人员（团队）累计发现高中危风险数（人工渗透测试漏洞，人工基线核查）少于 30 个的		-30 分
	人员出勤	1.4	工作人员在正常工作日按规定出勤，不得迟到、早退、无故旷工。出现违反日常规定的行为，按扣分标准进行扣分。	依据本协议要求，参考日常工作签到表。	-0.5 分/人次
	重要时期人员出勤	1.5	重要保障时期，额外增加人员提供招标范围系统安全保障评估，满足要求的，按加分标准		0.5 分/人 天 10 分/次
进度及交付物管控	资金支付材料提交	2.1	对于费用性支付，在支付当月 20 日前必须将该阶段支付相关凭证提交甲方；对于资本性支付，在支付前一个月 20 日前必须将该阶段支付相关凭证提交甲方。出现不及时提交的情况，按扣分标准进行扣分。	甲方出具整改通知书，且乙方没有实质性应答。	-2 分/次
	实施	2.2	按项目里程碑计划提交职责范围内	甲方出具整改通知	-2 分/份

	进度与交付物相符		符合甲方质量要求的交付物，乙方应每月提供入网安全评估月报，《入网安全评估报告》。出现提交不及时或者交付物质量问题，按扣分标准进行扣分。	书，且乙方没有实质性应答。	
	计划偏差	2.3	由于乙方责任导致项目里程碑计划延迟，提交入网安评申请后未及时开展入网安全测评工作，按扣分标准进行扣分。	甲方出具整改通知书，且乙方没有实质性应答。	二周内未完成初测： -2.5分/次； 一个月内未完成初测： -5分/次；
	项目周期性报告提交	2.4	按时提交项目月报。出现不按时提交的情况，按扣分标准进行扣分。	甲方出具整改通知书，且乙方没有实质性应答。	-1分/次
质量管控工作成效	内部通报	3.1	被广州局内部通报，非投标人主动发现的风险，按扣分标准进行扣分。	OA 通报	高危风险， -24分/次； 中危风险， -12分/次； 低危风险， -0.51分/次
	内部通报	3.2	被广州局内部通报，非投标人主动发现的，发送主机被控制、页面被篡改等网络安全事件，按扣分标准扣分。	OA 通报	主机被控制、系统被篡改，以管理员身份登陆集权系统

				的，数据库被拖库，-10分/次；以管理员身份登陆一般业务系统，登陆集权系统的，-5分/次。；
重要时期通报	3.3	在重要保供电、护网关键值守时期，被发现问题、通报的，按扣分标准进行扣分。	OA 通报	-2520 分
漏洞发现	3.4	主动发现漏洞风险，按加分标准加分。入网安评的，上限 20 分。	以乙方出具的测评报告，经第三方单位确认	高风险问题经第三方确认，加 2 分/个；每发现中风险问题经第三方确认，加 1 分/个；每发现低风险问题经第三方确认，加 0.5 分/个。相同类型风险问题累计可加至上限 105 分/类。招标范围系统，

				上限 10 分； 招标范围系 统所在网络 环境，不设 加分上限
风险 发现	3.5	主动发现招标范围系统所在网络环 境漏洞风险，按加分标准加分。	以乙方出具的测评报 告，经第三方单位确 认	控制主机， 篡改业务系 统，以管理 员身份登录 集权类系统 （4A、堡垒 机、G01、AD 域控等）， 数据库可整 体拖库，每 一个系统得 10 分；以管 理员身份登 录一般业务 系统，登录 集权类系 统，每个系 统得 5 分。
重保 加固 提升 及合 理化 建议	3.6	提出加固整改建议被呗招标方采 纳，并协助招标方实施落地，按加 分标准加分。加固建议包括但不限 于：蜜罐实施、防火墙策略整体调 优、入侵监测类设备误报整体调优 等整体性加固措施。	以乙方出具的加固报 告，经第三方单位确 认	10/次

	“三同步”管控	3.7	协助招标方审核招标范围系统“三同步”技术管控材料，协助招标方准确、按时开展定级备案，按加分标准加分	邮件通知	协助招标方审核“三同步”技术管控材料，0.5分/系统；协助招标方准确、按时开展定级备案，0.5分/系统。
	溯源分析	3.8	提供对招标范围系统应急响应过程中收集的可疑文件（如病毒、蠕虫、木马）的逆向分析和追踪溯源工作，每出具一份定位到攻击者身份的溯源报告的，按加分标准加分		5分/次
协同管控	变更审批合规	4.1	严格按照各项变更审批流程要求完成审批后实施变更	甲方出具整改通知书，且乙方没有实质性应答。	-2分/次
	出席会议	4.2	准时参加各项与项目相关的会议，如有问题事先应向会议组织者请假并获得同意	甲方出具整改通知书，且乙方没有实质性应答。	-1分/次
奖惩	奖励	5.1	甲方就本合同出具正式的表扬公告、信函等。	依据甲方出具的表扬表扬公告、信函等	加分项：5分/次；累计不超过10分。
	惩罚	5.2	上级通报。	以南方电网公司、广东电网公司相关发文和考核结果为依据。	若因进度或质量问题，导致甲方被

					南方电网通报，扣乙方10/次；若最终因此导致甲方被南方电网扣分的，追加扣10分。
--	--	--	--	--	--

十二、主要条款/参数优异性表格响应表

序号	技术规范书的要求	优于判定标准	投标响应内容	证明文件所在位置	是否偏离
1	区块链平台对接开发能力 评价标准： 满足要求：具备与区块链平台的实际对接开发经验，熟悉相关技术架构、节点部署要求及接口规范。提供上述对接开发经验证明材料的，视为满足基本要求。	具备与政务区块链平台的实际对接开发经验，熟悉相关技术架构、节点部署要求及接口规范。提供政务区块链平台对接开发经验证明材料的，视为优于基本要求。			优于/满足/负偏离
2	跨机构数据可信接入与链上核验场景项目经验。 具有上述相关实际项目经验，提供至少 1 个案例证明，视为满足基本要求。	具备政务领域相关实际项目经验，视为优于基本要求。			优于/满足/负偏离
3	对本项目所引用的区块链相关标准具有深度理解和实施经验。参与区块链标	标准起草单位排名前三，视为优于要求。			优于/满足/负偏离

	准制定，视为满足要求。				
--	-------------	--	--	--	--

十三、技术条款/技术参数点对点应答表

序号	技术规范书的要求	投标响应内容	证明文件所在位置	是否偏离
1	满足对依据的标准和规范的理解：见 1.1			满足/负偏离
2	满足对项目要求的理解：见 2.1			满足/负偏离
3	满足对项目背景的理解：见 2.2			满足/负偏离
4	满足对建设目标的理解：见 2.3			满足/负偏离
5	满足对建设范围的理解：见 2.4			满足/负偏离
6	满足对项目准备工作的理解：见 3.1			满足/负偏离
7	满足对项目准备工作的理解：见 3.1			满足/负偏离
8	满足对业务需求的理解：见 3.5.1			满足/负偏离
9	满足对功能需求的理解：见 3.5.2			满足/负偏离
10	满足对应用功能的理解：见 3.5.3			满足/负偏离
11	满足对技术架构要求的理解：见 3.6.1			满足/负偏离
12	具有清晰的项目知识转移与培训计划，能			满足/负偏离

	够提供详细的技术文档交付标准和运维体系建设经验。			
--	--------------------------	--	--	--

十四、服务团队优异性表

序号	技术规范书的要求	优于判定条件	投标响应内容	证明文件所在位置	是否偏离
1	团队须具备区块链平台开发及跨链对接的实际项目经验,核心成员能够提供其参与经第三方验证或已落地实施的区块链相关项目的证明材料。	在满足基准要求前提下,有市级及以上区块链项目经验,视为优于要求。			优于/满足/负偏离
2	区块链相关专利能力评价标准: 提供 2 项区块链或链上应用相关已授权专利,视为满足要求。	提供已授权区块链专利 4 项及以上,视为优于要求。			优于/满足/负偏离

十五、一般服务团队条款/参数应答表

序号	技术规范书的要求	投标响应内容	证明文件所在位置	是否偏离
1	团队成员资质要求: 计算机技术与软件专业技术资格中级或以上证书不少于 2 人			满足/负偏离
2	投标人须配置不少于			满足/负偏

	5 人的项目实施团队，团队成员须覆盖项目管理、区块链架构、软件开发、测试等关键角色，各角色须有明确的人员配置及职责分工			离
3	具备本地化服务能力，能够为项目实施及运维阶段提供及时响应的现场支持。			满足/负偏离
4	满足对服务团队及服务能力的理解：见第六章			满足/负偏离
5	满足对服务承诺的理解：见第九章			满足/负偏离

十六、评价申辩

如果投标人不认可服务评价结果，可以在结果公布后 3 个工作日内向招标人提出申辩，最终的评价结果以双方协商后的结论为准。

十七、违约责任

17.1 合同终止条款

若出现以下情况之一的，招标人有权终止合同并追究相关法律责任。

- 1、合同履行期间内，累计出现一次一级安全事件。
- 2、合同履行期间内，累计出现两次二级安全事件。
- 3、合同履行期间内，累计出现三次三级安全事件。

4、招标人有权对投标人项目参与人员进行面试或者考试（面试或者考试范围为项目工作内容），发现驻场人员资质或工作经验造假情况。

5、投标人项目参与人员未经招标人书面同意而参加其他项目工作，或未经招标人书面同意更换项目参与人员数量超过总数比例 20%。

6、经招标人发出部门整改通知书 3 次或以上，或广州局整改通知书 2 次或以上。

17.2 评分扣款说明

在合同服务期结束前，招标人按照本协议对投标人的服务进行服务评价。如果评价结果低于 80 分，将视为投标人违约，招标人向投标人支付最后一期合同款项时，按照以下规则扣减一定比例后支付：

评价分数低于 80 分且不低于 75 分，则扣减合同总额的 5%，具体金额以合同为准；

评价分数低于 75 分且不低于 70 分，则扣减合同总额的 10%，具体金额以合同为准；

评价分数低于 70 分且不低于 65 分，则扣减合同总额的 15%，具体金额以合同为准；

评价分数低于 65 分，则扣除合同总额的 20%，具体金额以合同为准。

在本合同在执行过程中，如存在不确定因素导致投标人未按约定实施时长，则招标人有权根据实际工作量签订补充协议延长服务期或扣减相应合同金额。

十八、效力说明

本技术规范书作为招标方案的附件，与招标方案具有同等法律效力。

（以下无正文）