ICS 35.210
CCS L

中华人民共和国国家标准

GB/T XXXXX—XXXX

量子计算服务平台
第 1 部分：架构与功能要求

Quantum computing service platform—
Part 1: architecture and functional requirements

（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。

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件是GB/T XXXXX《量子计算服务平台》的第1部分。GB/T XXXXX已经发布了以下部分：

——第1部分：架构与功能要求

——第2部分：性能评估

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国量子计算与测量标准化技术委员会（SAC/TC 578）提出并归口。

本文件起草单位：中国信息通信研究院、中国科学技术大学、中移(苏州)软件技术有限公司、中电信量子信息科技集团有限公司、华翊博奥（北京）量子科技有限公司、北京玻色量子科技有限公司、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、科大国盾量子技术股份有限公司、合肥国家实验室、中国人民解放军网络空间部队信息工程大学、深圳量旋科技有限公司、北京交通大学、中国科学院软件研究所、中国长城科技集团股份有限公司、广东国腾量子科技有限公司、中国信息安全研究院有限公司、东南大学、中国科学技术大学上海研究院、中国标准化研究院、上海交通大学、中科酷原科技（武汉）有限公司、上海图灵智算量子科技有限公司、中国计量大学、青岛大学、合肥弈维量子科技有限公司、本源量子计算科技（合肥）股份有限公司、北京中科弧光量子软件技术有限公司、济南量子技术研究院、郑州大学、量子科技长三角产业创新中心、无锡光子芯片联合研究中心。

本文件主要起草人：　张萌、王敬、赖俊森、梁福田、李明悦、刘勇、赵文定、陈亮、吴婷、李东东、唐世彪、吴玉林、姚金阳、王肖斌、郭聪、毛志超、高奇、文凯、任爽、高丁超、于春霖、曹明明、周朋、吕启闻、郭邦红、王增斌、黄智国、李鹤、姚飞、徐洋、康键、金贤敏、唐豪、汤彪、付卓、石志全、刘国珍、杨林、谭爱红、安斯光、闫艳、徐华、赵勇杰、窦猛汉、方圆、应圣钢、丁锦涛、楼华哲、周飞、王超凡、郑明睿、卢丽芳、侯一凡、戚旭衍、刘福东、于哲、郑留帅、魏志猛。

引 言

目前量子计算硬件尚无法满足个人用户本地部署的要求。为了让更多研究人员和行业用户参与到量子计算硬件、软件、算法和应用的研究和探索当中，近年来量子计算服务平台逐渐成为量子计算服务输出的主要形式。用户依托经典的信息网络基础设施，访问云端的量子计算处理器。用户编写的量子线路或程序通过网络提交给云端的经典服务器进行编译和下发，在真实的量子处理器硬件或量子资源经典模拟器上运行，运行结果最终反馈给用户，实现运算的闭环运行。目前，国内外许多研究机构和企业陆续发布自己的量子计算服务平台，以此推动量子计算产业落地和生态建设已成为业界共识。制定量子计算服务平台相关国家标准，通过建立统一的功能架构，推动国内量子计算服务平台功能完善和性能提升，增强量子计算硬件与经典计算硬件、云平台的互通性与互操作性。

GB/T XXXXX《量子计算服务平台》旨在规定量子计算服务平台的架构、功能要求、技术参数、测试方法、可靠性试验、检验规则等要求，依照系统主要功能模块划分，标准目前拟由两个部分构成。

——第1部分：架构和功能要求。规定量子计算服务平台的架构和功能要求等要求。

——第2部分：性能评估。规定量子计算服务平台性能评估体系、评价指标和测试方法等要求。

随着技术与产业发展，未来可能包含更多部分。

量子计算服务平台 第1部分：架构与功能要求

1 范围

本文件描述了量子计算服务平台的架构和功能要求，包括量子计算服务平台服务模式和功能架构、接入门户功能要求、应用服务功能要求、平台服务功能要求、基础设施服务功能要求、资源管理功能要求、虚拟资源功能要求、物理资源功能要求、外围基础设施功能要求、运营管理功能要求和安全保障功能要求等。

本文件适用于量子计算服务平台及其相关领域的研发、应用和测试等工作。

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。

GB/T 37736-2019 信息技术 云计算 云资源监控通用要求

GB/T 42565-2023 量子计算 术语和定义

GB/T XXXXX-202X 量子计算系统性能测试方法

3 术语和定义

GB/T 42565-2023界定的以及下列术语和定义适用于本文件。

3.1

量子计算机 quantum computer

一种遵循量子力学规律进行数学和逻辑运算、存储及处理量子信息的物理装置。

[来源：GB/T 42565-2023，4.10]

3.2

门型量子计算机 gate-based quantum computer

通过定义量子门并依靠量子门序列来完成量子计算任务的量子计算机。

3.3

非门型量子计算机 Non-gate-based quantum computer

针对特定的物理系统或量子现象进行模拟来完成某类特定的问题的量子计算机。

3.4

量子计算服务平台 quantum computing service platform

实现量子计算资源按需提供与服务化交付的软硬件集合，由量子计算机硬件资源、量子计算服务、资源管理与调度功能、以及辅助的经典信息通信基础设施（包括计算、存储、通信网络等）等构成。

[来源：GB/T 42565-2023，6.1，有修改]

3.5

量子资源经典模拟器 classical simulator for quantum circuit

利用经典计算方式来仿真模拟量子系统演化的设备。对于模拟非门型量子计算机的设备，可简称为经典模拟器。

[来源：GB/T 42565-2023，4.19，有修改]

4 缩略语

下列缩略语适用于本文件。

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

CNOT：受控非（Controlled NOT）

CPU：中央处理器（Central Processing Unit）

CSP：内容安全策略（Content Security Policy）

CSRF：跨站请求伪造（Cross-Site Request Forgery）

DDoS：分布式拒绝服务（Distributed Denial of Service）

DoS：拒绝服务（Denial of Service）

FIFO：先进先出（First Input First Output）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

IDE：集成开发环境（Integrated Development Environment ）

IDS：入侵检测系统（Intrusion Detection System）

IP：互联网协议（Internet Protocol）

IPSec：互联网安全协议（Internet Protocol Security）

Q-IaaS：量子基础设施即服务（Quantum Infrastructure as a Service）

Q-PaaS：量子平台即服务（Quantum Platform as a Service）

Q-SaaS：量子软件即服务（Quantum Software as a Service）

SQL：结构化查询语言（Structured Query Language）

SSL：安全套接层（Secure Sockets Layer）

XSS：跨站脚本攻击（Cross-Site Scripting）

5 量子计算服务平台功能架构

5.1 概述

量子计算服务平台的功能架构如图1所示，主要由接入门户、应用服务、平台服务、基础设施服务、资源管理、虚拟资源、物理资源、外围基础设施、运营管理、安全保障等功能模块组成。图中虚线框表示可选功能模块。对于不同服务模式的量子计算服务平台，其支持的功能模块有所差异。量子计算服务平台的服务模式可参考附录A。

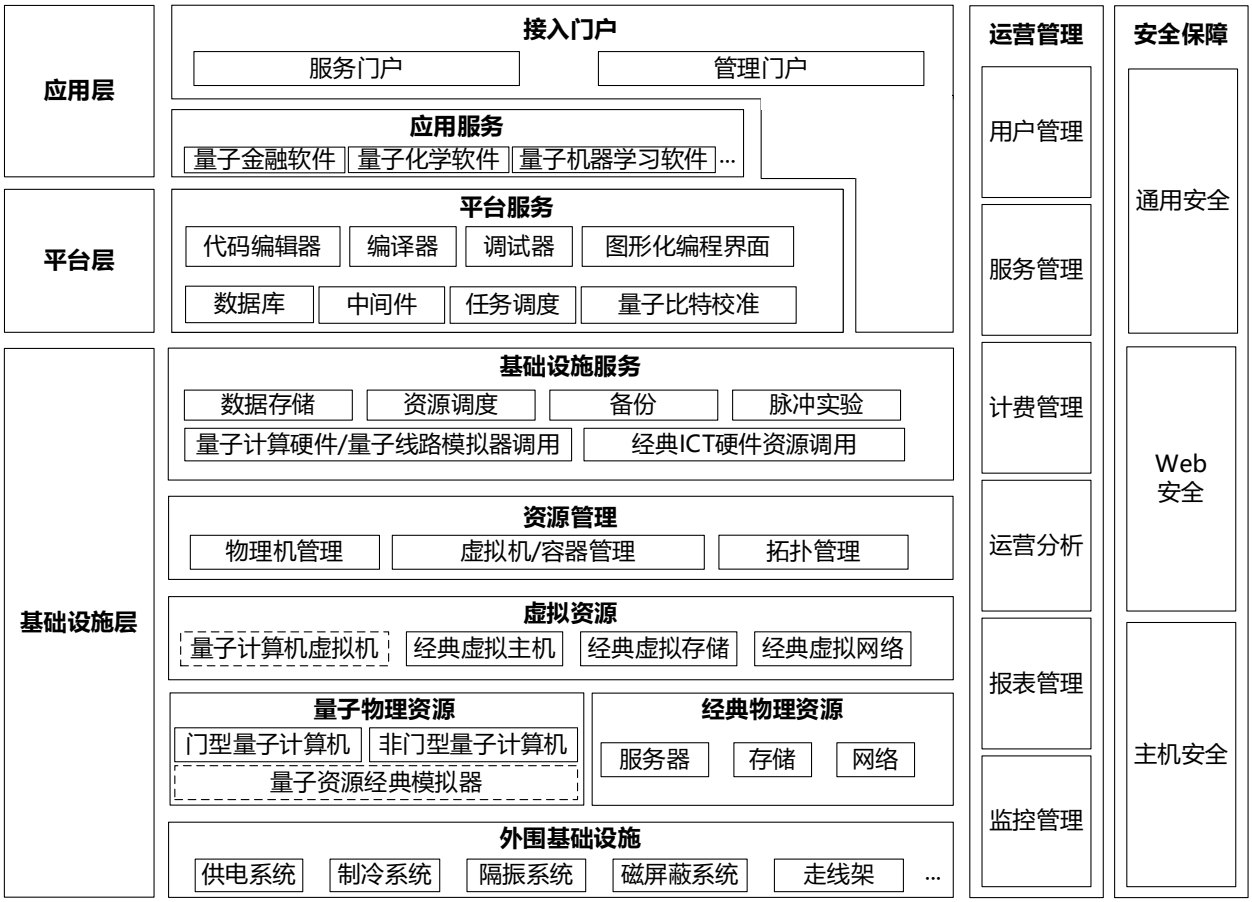


图1　量子计算服务平台功能框架图

5.2　应用层

应用层由接入门户和应用服务功能模块组成：

a)　接入门户功能模块：为用户或管理人员提供服务平台的操作界面，又可以细分为服务门户和管理门户两个子功能模块。

- 服务门户功能模块主要面向用户开放，提供用户账号注册、登录、注销、订购/取消服务等功能；
- 管理门户功能模块主要面向管理运维人员开放，提供服务和服务目录的新建、修改、删除等功能，同时提供用户信息、报表、日志等的查询等功能。

应用服务功能模块：为用户提供量子计算应用软件服务。

5.3　平台层

平台层包含平台服务功能模块，主要提供图形化/代码编程开发、程序编译、程序调试、任务调度、量子比特校准等功能。同时也应提供数据库、中间件等必要的经典云服务平台功能。用户通过开发平台进行程序开发和运行，任务调度模块根据用户已订购的物理或虚拟资源的负荷情况对用户提交的任务进行队列调度。由于目前量子计算硬件性能尚不稳定，需要定期进行校准，平台服务功能模块还应为用户或管理员提供比特校准功能，校准可采用在线或离线方式，可通过手动或自动形式完成。

5.4　基础设施层

基础设施层由基础设施服务、资源管理、虚拟资源、物理资源和外围设施等功能模块组成：

a) 基础设施服务功能模块：主要提供数据存储、资源调度、备份、硬件资源调用等功能。基础设施服务功能模块既可以独立为用户提供基于量子计算硬件的服务，如量子计算硬件的调用或租赁等；也可以实现平台层与底层硬件的桥接，如用户任务在经典和量子资源池中的调度等；
b) 资源管理功能模块：主要提供物理机管理，虚拟机/容器管理和拓扑管理等功能。资源管理功能模块为管理员提供资源的新增、统一纳管、信息修改、虚拟化/容器化、删除等全生命周期管理功能；
c) 物理资源功能模块：主要提供量子计算机硬件（门型量子计算机或非门型量子计算机）、量子资源经典模拟器、经典服务器、经典存储设备、经典网络等硬件。虚拟资源功能模块主要提供经典虚拟机或容器等功能；
d) 外围设施功能模块：主要为量子计算硬件正常运行提供支撑保障，包括但不限于供电系统、制冷系统、温控系统、隔振系统、磁屏蔽系统、走线架、除尘洁净系统（超净间）、防静电等；
e) 物理资源功能模块又分为量子物理资源和经典物理资源两个子功能模块。

5.5 运营管理功能模块

主要提供用户管理、服务管理、计费管理、运营分析、报表管理和监测管理等功能。

5.6 安全保障功能模块

主要提供通用安全、主机安全和Web安全等功能。其中通用安全功能模块主要提供用户认证、授权管理、信息安全、数据安全、业务逻辑、API安全、日志留存和业务系统加固等功能。主机安全功能模块主要提供量子计算机安全、经典服务器安全、网络安全和虚拟化环境安全等功能。Web安全功能模块主要提供垂直越权漏洞防护、跨站脚本攻击防护、SQL注入漏洞防护、平行越权漏洞防护、跨站请求伪造漏洞防护等功能。

6 量子计算服务平台功能要求

6.1 接入门户功能模块

6.1.1 服务门户功能

服务门户模块为用户提供基本的接入、认证、服务订购等功能。服务门户模块应支持以下功能：

a) 用户通过服务门户查看已授权的服务目录；
b) 用户通过服务订购功能生成服务订单；订单生成后支持订单总价显示，为用户提供提交订单、暂存订单、取消订单等功能；
c) 对用户订购服务的资源规格、计费模式等参数进行变更；
d) 服务退订功能。服务退订支持手工退订和自动退订两种类型。用户可通过手工退订功能在线删除所购买服务。自动退订功能可自动删除过期服务；
e) 服务售后功能。包括但不限于技术支持、故障定位与修复、投诉处理与反馈等；
f) 资源信息展示功能，提供用户订购服务所包含的计算、存储和网络等资源的性能监控、统计分析和告警管理；
g) 信息查询功能，用户能够通过服务门户查询和修改用户资料，如用户名称、联系方式等。用户能够通过服务门户查询订购服务所包含的资源信息。用户可在服务门户上查询历史账单和当前账单；
h) 为用户提供产品介绍，为用户提供产品信息，通知公告等信息浏览及查询；
i) 为用户提供快捷、安全的网站登录功能及密码修改、找回功能。

服务门户模块宜支持以下功能：

a) 计算资源操作，提供订购服务所包含的虚拟机/容器运行控制（启动、关闭、重启等）、备份恢复等功能；
b) 订单质疑和售后功能，其流程可参考附录 B。

6.1.2 管理门户功能

管理门户模块为服务平台管理运维人员提供账号接入、基本信息查询修改等功能。管理门户模块应支持以下功能：

a) 对服务的定义、修改、删除和查询，以及服务目录的生成、发布、修改、删除、查询和导入导出等操作；
b) 对资源的管理，包括资源池创建、状态设置（如启动服务、暂停服务、终止服务等）、资源状况信息获取及展示等操作；
c) 提供与资源部署调度模块所要求的各项功能相对应的门户操作界面；
d) 对服务实例的创建、变更、终止等操作，以及对服务实例基本信息等进行操作与查询；
e) 对各类资源的数量、状态、属性的监控；
f) 用户的创建、删除，用户信息修改、密码修改、密码重置、用户状态设置、用户信息查询等操作；
g) 对各类资源的统计数据搜集、展示及统计报表输出等操作；
h) 对系统记录日志信息的展示，包括操作日志、系统日志、计算日志等；
i) 为管理员提供快捷、安全的网站登录功能及密码修改、找回功能。

6.2 应用服务功能模块

应用服务模块为用户提供量子计算应用软件服务，用户通过web浏览器或移动应用程序以互联网接入的方式使用量子计算应用程序，而无需对量子计算应用程序进行更新与维护。应用服务模块应支持以下功能：

a) 用户通过应用服务软件（或模块）提供无代码或低代码的量子计算应用服务，如量子机器学习、量子组合优化、量子化学模拟、量子金融等；用户通过加载待计算数据或导入待计算模型等简单操作即可完成特定问题的求解；对于待计算问题，应提供问题模型加载（或导入）的模板，并支持计算过程及结果的可视化；
b) 用户基于量子计算应用算法库自主开发量子计算应用程序，服务平台为用户提供必要的应用算法接口、量子线路接口或代码实例，指导用户针对特定问题开发个性化的应用程序。

注：对于 Q-PaaS 和 Q-IaaS 平台，应用服务层功能模块为可选。

6.3 平台服务功能模块

平台服务模块借助量子计算服务平台提供商提供的工具在基础设施（如量子计算机硬件和必要的辅助经典硬件）上部署用户创建的或已存在的量子计算应用。其中，这里的平台工具包括但不限于应用开发编程语言及工具（图形化编辑工具、代码编辑器、调试器、编译器等）、数据库、中间件等。平台服务模块应支持以下功能：

a) 对于提供门型量子计算机的服务平台，支持通过 IDE、低代码或无代码等提供可视化、图形化、可拖拽等配置方式进行量子线路创建和运行，运行结果展示；对于提供非门型量子计算机的服务平台，支持通过 IDE、低代码或无代码、导入式等提供可视化、图形化、可拖拽等配置方式创建量子计算任务，支持运行和结果展示；
b) 对于提供门型量子计算机的服务平台，支持通过编程语言实现量子线路创建和运行，支持运行结果返回和查询；对于提供非门型量子计算机的服务平台，支持通过编程语言创建量子计算任务，支持运行和结果返回；

c） 对于提供门型量子计算机的服务平台，支持参数化线路的创建、赋值、运行，运行结果返回和查询；对于提供非门型量子计算机的服务平台，支持参数化量子计算系统进行参数编辑、模型选择和运行，运行结果返回和查询；

d） 经典-量子混合编程功能，其中经典编程功能包括但不限于支持各种经典数据类型（如整数、浮点数、字符、布尔值等）并允许用户使用变量来存储和操作这些数据、支持各种经典算术和逻辑操作符（如加、减、乘、除、与、或、非等）以及控制结构（如条件语句、循环语句等）、支持经典函数的定义与调用等；支持在经典编程中调用量子任务并将量子计算结果返回经典程序；

e） 量子程序的编译和运行，支持运行结果的返回和查询；

f） 提供开发模板的能力和指导，以便于用户快速理解和实施开发；

g） 调试和测试的沙箱环境、测试工具和脚本调试等调试手段和方式；支持代码调试功能，用于在代码执行过程中逐行执行和检查代码，如设置经典程序的断点、观察变量的值、跟踪函数调用和返回等功能。

h） 统一的数据库访问服务，屏蔽底层的异构数据库特性，为上层应用提供了简单方便的数据库访问接口；

i） 提供中间件，实现应用软件和底层异构硬件之间的解耦，屏蔽底层硬件的复杂性。

j） 任务队列调度功能，支持按照先入先出（FIFO）方式调度任务；

k） 任务的分解和调度，将经典计算部分分配给经典服务器，将量子计算部分分配给量子计算机或量子资源经典模拟器；支持不同计算单元返回结果的整合；

l） 量子计算机的在线或离线错误检测和校准功能。

平台服务模块宜支持以下功能：

a） 单个量子计算机物理机上并行执行多个量子计算任务。

b） 对于提供门型量子计算机的服务平台，支持量子线路优化功能。

c） 对于提供非门型量子计算机的服务平台，支持通过算法把计算规模大的任务拆分成小规模任务进行并行或者迭代计算，从而允许用户提交并运行问题规模大于物理机量子比特数目的计算任务。

d） 对于支持多种物理体系类型量子计算机资源的服务平台，支持用户指定任务运行所需要的量子计算机资源；支持根据任务特征为用户自动调度并分配更合适的量子计算机资源；支持根据量子计算资源状态为用户任务自动调度并分配合适的量子计算机资源。

e） 多种灵活调度模式，如最短作业优先、最短剩余时间优先、多级反馈队列以及基于优先级的层次化调度等方式。

注：对于 Q-IaaS 平台，平台服务层功能模块为可选。

6.4 基础设施服务功能模块

基础设施服务模块向用户提供量子计算基础资源（如量子计算硬件和必要的辅助经典硬件），用户在上面部署和运行任意的应用程序，而无需直接管理和控制底层硬件资源。基础设施服务模块应支持以下功能：

a） 对资源的生命周期和资源信息的监控和修改；

b） 根据上层应用和服务的负载情况，手动分配物理和虚拟资源；

c） 对不同资源域实现不同的监测、管理策略；

d） 资源绑定，支持虚拟机以专享方式使用特定 CPU 内核、内存大小、存储设备等；

e） 资源优先级设定，优先级至少包括高、中、低三个级别；

f） 虚拟机迁移操作；

g） 虚拟机/容器的负载均衡、高可用、节能管理；

h） 虚拟机挂载文件系统；

i） 虚拟机重装系统、切换系统、根据虚拟机创建系统镜像等；

j） 数据的存储与备份，数据存储要求可参考附录 C。

基础设施服务层宜支持基于脉冲级的测控信号编辑、产生、运行及结果返回。

6.5 资源管理功能模块

6.5.1 物理机管理功能

物理机管理模块为管理员或用户提供服务平台上物理资源（包括真实的量子计算硬件、经典硬件设备等）的统一纳管功能，如物理资源信息的获取、配置、修改、查询，以及物理资源的计量等功能。物理机管理模块应支持以下功能：

a） 对量子计算服务平台资源域内分布在不同物理机房的可管理和调度的量子计算机和经典物理机（如服务器、存储器、网络设备等）分别进行统一管理；

b） 获取纳管的物理机的信息，如资产信息、硬件信息、性能信息、工作状态等；

c） 显示所管理的物理机的清单列表，并能动态更新和维护管理；

d） 对纳管的物理机进行多维度的查询；

e） 对所纳管的物理机进行远程的、统一的、可批量执行的配置，如软件安装，虚拟机创建及其操作系统的安装，IP 地址配置，存储空间的配置，域管理，用户管理，日志管理，共享文件服务配置等；

f） 对纳管的物理机进行统一管理，包括对配置信息的管理、严格的变更控制、自动化的变更管理、对管理操作全面记录等功能；

g） 确定的、计算简单的量子计算资源计量方法，如：门型量子计算机按量子比特数等计量量子计算资源，计量方法应符合 GB/T XXXXX-202X（量子计算系统性能测试方法）中的要求；非门型量子计算机按希尔伯特空间大小、支持求解问题规模大小等计量量子计算资源；

h） 确定的经典资源计量方法，如：按 CPU 个数、内存等计量经典服务器资源；按存储容量、存储读写带宽等计量经典存储资源；按网络入站出站带宽、入站出站流量等计量经典网络资源。

6.5.2 虚拟机/容器管理功能

虚拟机/容器管理模块为管理员或用户提供虚拟机的创建、配置、生命周期管理、快照与备份等相关功能。虚拟机/容器管理模块应支持以下功能：

a） 通过专业虚拟化管理软件的接口实现对分布在不同物理机房内虚拟机的统一管理；

b） 虚拟机/容器生命周期管理，主要包括虚拟机/容器创建、运行控制、修改、删除等；

c） 对虚拟机/容器进行基本的配置；

d） 虚拟机/容器的批量部署；

e） 通过快照的方式把虚拟机/容器某一时刻的状态保存下来，并进行新虚拟机/容器的创建或者用户数据恢复。

注：本节功能要求仅适用于支持虚拟机/容器功能的量子计算服务平台。

6.5.3 拓扑管理功能

拓扑管理模块为管理员提供资源拓扑的查询与配置功能。拓扑管理模块支持以下功能：

a） 各类资源节点拓扑关系的查询，包括但不限于物理设备、虚拟资源之间的连接关系等，并以图形化的方式展示；对拓扑视图进行编辑，包括但不限于对资源节点的添加、配置、删除等操作；

b） 量子计算机内部量子比特之间拓扑关系的动态监测和查询，包括但不限于门型量子计算机量子比特之间的物理连接关系及量子比特之间双比特门保真度、非门型量子计算机量子比特之间的连接关系以及耦合精度等，并以图形化的方式展示。

6.6 虚拟资源功能模块

虚拟资源层将服务平台上的物理资源（如经典服务器、存储器、网络等）进行虚拟化或容器化，形成资源池，按需动态地分配给用户，并保证虚拟机或容器之间的隔离特性。虚拟资源模块应支持以下功能：

a） 对经典物理资源的虚拟化或容器化；

b） 虚拟机或容器之间的隔离特性；

c） 虚拟化资源或容器化资源的弹性伸缩。

注：本文件对量子计算硬件的虚拟化功能暂不作要求。

6.7 物理资源功能模块

物理资源功能层为量子计算服务平台提供量子计算机硬件和必要的经典物理资源。量子计算机硬件可包括门型量子计算机或非门型量子计算机。除真实的量子计算硬件外，量子计算服务平台还可提供量子资源经典模拟器，为用户提供量子算力模拟、算法调试等功能。量子计算服务平台还应提供必要的经典物理资源（如服务器、存储器、网络设备等）。物理资源模块应支持以下功能：

a） 量子计算机或量子资源经典模拟器的接入、占用、释放和状态查询；

b） 对于提供门型量子计算机的服务平台，支持量子计算机上一定深度和宽度的量子线路的建立、运行和结果输出；对于提供非门型量子计算机的服务平台，支持支持量子计算机上一定规模的量子计算任务的建立、运行和结果输出；

c） 对于提供门型量子计算机的服务平台，支持量子资源经典模拟器上一定深度和宽度的量子线路的建立、运行和结果输出，量子资源经典模拟器支持全振幅、部分振幅、单振幅或稳定子量子资源经典模拟器后端，支持含噪声量子资源经典模拟器后端；对于提供非门型量子计算机的服务平台，支持经典模拟器上一定规模的量子计算任务的建立、运行和结果输出；

d） 对于提供门型量子计算机的服务平台，支持提供完备和通用的量子逻辑门集合，量子逻辑门的完备性可参考附录 D；

e） 必要的经典资源（如经典服务器、虚拟服务器/容器、经典存储设备、经典网络设备等）的占用、使用和释放。

物理资源功能层可选支持分布式容器化的量子资源经典模拟器，即利用服务平台上资源实现量子模拟规模动态扩展，组合单节点计算资源形成分布式计算集群，实现中/大规模量子程序模拟执行。

6.8 外围基础设施功能模块

外围基础设施主要为量子计算硬件正常运行提供温度、电力、振动、洁净度、湿度、电磁屏蔽等保障。

注：本文件对外围基础设施层暂不作要求。

6.9 运营管理功能模块

6.9.1 用户管理功能模块

用户管理模块主要提供用户的注册、修改、注销、分类分级、授权等功能。用户管理模块应支持以下功能：

a） 用户的注册、注销，用户信息修改、密码修改、密码重置、用户信息查询等操作；

b) 对用户分类并分级管理，支持将管理员划分为多个用户组，不同用户组的用户拥有不同的资源权限；
c) 权限管理，对量子计算服务平台功能架构中的功能进行分层、统一访问控制；
d) 对操作权限的分配和用户与特定范围的资源的绑定，资源范围支持域级别的划分；
e) 用户创建 API 调用令牌。
f) 用户签署隐私保护申明，签署 cookies 访问协议。

6.9.2 服务管理功能模块

6.9.2.1 服务目录管理功能

服务目录管理模块主要为管理员提供服务目录及其中的服务产品的创建、修改、下线、删除等操作，为管理员或用户提供服务目录的查询功能。服务目录管理模块应支持以下功能：

a) 通过服务目录模块进行服务的定义和创建，将能够提供的资源以服务的形式向用户提供；
b) 通过服务目录模块正式发布一项或多项服务；
c) 通过服务目录模块将一项或多项服务进行下线；
d) 修改各类服务的相关属性，如服务名称、服务权限、服务版本和配置计算资源等；
e) 服务设计者和终端用户查询各类服务目录及其相关属性；
f) 删除一个或多个服务。

6.9.2.2 服务实例管理功能

服务实例管理模块主要为用户或管理员提供服务目录中服务实例的订购、激活、修改、查询、监控、暂停、注销等全生命周期管理。服务实例管理模块应支持以下功能：

a) 按照服务目录所定义的服务内容生成对应的服务实例，并能够完成服务实例的申请、正式创建、挂起、激活、修改、查询、注销、监测等生命周期管理及工单管理功能；
b) 在用户订购服务后，能够按照服务目录的规定，预生成相应的服务实例，并向资源管理域相关模块下发相应的资源部署指令；
c) 在收到资源部署就绪指令后，启动监控、告警等外部系统，将预生成的服务实例升级为正式创建状态，并发布服务；
d) 由终端用户主动暂停服务，并将服务实例挂起；
e) 由终端用户激活已挂起的服务实例；
f) 手动或自动修改服务实例的各个属性，如服务实例申请运行时长、服务实例状态等；
g) 服务设计者和终端用户查询各个服务实例及其相关属性；
h) 注销一个或多个服务实例；
i) 服务高可用部署策略，如多区域、多节点部署等；
j) 实时监测各个服务实例的运行状态，能够提供必要的提示和告警。

6.9.3 计费管理功能模块

计费管理模块为管理员或用户提供计费信息的收集、话单的生成、查询等功能。计费管理模块应支持以下功能：

a) 收集各个功能组件产生的相关计费信息，生成满足量子计算服务平台服务计费要求并满足外部计费结算系统格式要求的话单；
b) 形成批价及优惠后的量子计算服务平台服务话单；
c) 原始话单和批价话单信息查询统计功能；

计费管理模块宜支持根据外部计费系统的格式要求对原始话单进行格式化，满足外部计费系统的结算要求。

6.9.4 运营分析功能模块

运营管理模块主要为管理员提供用户、服务目录及实例、订单等基本信息的查询、监控、统计分析等功能。运营管理模块应支持以下功能：

a) 对客户的行业分布、订购情况和实际使用情况等进行统计分析，包括但不限于客户主要行业分布、客户订购资源类型、各种资源类型使用时长等；
b) 对量子计算服务平台服务目录、订单处理、服务保障等进行监控管理和统计分析，包括但不限于服务目录使用率、服务模板使用率、客户自定义服务模板使用情况、客户订单处理效率、客户订单成功率、服务故障情况等。

6.9.5 报表管理功能模块

报表管理模块主要为管理员或用户提供报表的统计、生成、展示、导出等功能。报表管理模块应支持以下功能：

——提供各类资源、信息的数据搜集、存储以及展示，提供各种统计报表和分析报告。

6.9.6 监测管理功能模块

监测管理模块主要为管理员和用户提供各类设备的性能监测、告警收集、故障定位等功能。监测管理模块应支持以下功能：

a) 对各类资源、设备的工作状态和关键性能指标进行监测和更新；
b) 对设备任务队列进行监测；
c) 捕获各类设备的告警信息，进行故障诊断及定位分析；
d) 配置告警通知，如手机、邮件通知等。

6.10 安全保障功能模块

6.10.1 通用安全功能

6.10.1.1 用户认证

用户认证模块主要通过身份认证功能保障用户账号安全以及平台系统安全。用户认证模块应支持以下功能：

a) 对登录系统的用户进行身份识别，认证系统根据客户的身份和授权，安全地接入业务平台；
b) 常见的安全认证方式，如口令认证、数字证书等；
c) 口令认证方式下，支持口令长度及复杂度验证、提供对用户口令全生命周期控制功能，确保口令和私有密钥的安全性；
d) 用户的密码通过密码加密和密码校验技术进行加密存储，从而避免明文密码泄露、缓解彩虹表撞库等密码安全问题。前端密码经过加密、校验处理后，传输到后端服务器验证，后端对得到的加密密码二次校验处理，将其存储至数据库，或是与数据库中用户存储的密码比较是否一致；
e) 接入熔断机制，当系统短时间内遭受大量并发攻击请求时，应当触发熔断机制，防止整个系统瘫痪；
f) 自定义账号安全策略功能。如：最大连接数控制功能等。

6.10.1.2 授权管理

授权管理模块通过设置和校验用户对特定资源或特定操作的权限来保障用户及服务平台系统的安全。授权管理模块应支持以下功能：

a) 对设备资源（含虚拟机资源/容器、存储资源）的管理；对应用系统资源（管理平台、用户门户）的管理；对资源中角色的管理、对账号和资源间授权关系的管理；
b) 权限控制功能，根据不同用户角色，设置相应权限，用户的重要操作都做相应的日志记录以备查看，没有权限的用户禁止使用系统。当用户账户发生变更时，已经颁发的权限证书应当做失效处理；
c) 根据用户、用户组、用户级别的定义来对资源的访问进行集中授权；
d) 动态创建、删除和修改角色，形成新的权限集合分配给系统用户，以控制系统用户的权限；
e) 对常见各类操作的细颗粒度授权策略；
f) 对访问途径的严格控制：如通过 Web 界面能完全执行的功能，就不再提供其他的访问途径，如命令行的访问。

6.10.1.3 信息安全

信息安全模块通过对组件配置信息、源代码、账号口令等敏感信息的加密、限制操作等手段来保障用户及服务平台系统的安全。信息安全模块应支持以下功能：

a) 对网站后台敏感信息的保护，不在前端显示或存储，如网络目录、数据库、中间件及框架版本等；
b) 对网站各组件版本和配置信息的保护，请求中不包含组件信息，删除网站组件的默认页面，同时修改默认账号和报错页面；
c) 网站目录中不存放敏感文件；
d) 对端数据的保护，后端根据具体业务需求只推送必要的展示数据至前端；
e) 对源代码的保护，不将项目及产品代码管理平台文件打包至项目文件中；
f) 对账号口令的保护，不将明文账号口令写入日志、配置文件、代码、代码注释等。

6.10.1.4 数据安全

数据安全模块通过对数据进行加密存储、加密传输、访问权限设置、容灾备份等操作，来保障用户和服务平台系统的安全。数据安全模块应支持以下功能：

a) 数据加密存储，服务层自身管理数据、用户数据、业务数据等都必须加密存储；
b) 数据通信加密，对量子计算服务平台管理系统上流通的数据进行加密通信，用户上传及下载的数据也要求加密通信。加密协议可以是 SSL、IPsec 等；
c) 数据访问权限和认证管理，用户只能访问自己的数据；
d) 数据存储支持容灾能力，具备多副本存储能力，定期对数据进行多机备份，防止当系统异常重启、崩溃时造成数据丢失，无法还原。数据库不能在公网下进行暴露，并且创建访问白名单；
e) 数据备份和恢复过程的管理和安全性，用户只能对自己的数据进行备份和下载，备份过程保证安全；
f) 数据分类和隔离，最终用户的数据，应用服务的数据，管理数据属于不同的数据，需要隔离存放并被赋予分开的管理权限。

6.10.1.5 业务逻辑安全

业务逻辑安全模块通过校验应用程序或业务系统功能和流程的完整性、与设计预期的符合程度等来保障用户和服务平台系统的安全。业务逻辑安全模块应支持以下功能：

a) 业务逻辑的后端校验，所有校验需在后端进行校验，不允许只在前端进行校验，如产品价格、产品规格、订购时长、用户认证信息等重要参数需在后端做合法性验证，非法参数则拒绝处理，

避免产生产品重复订购、0 元购、可订购超过购买数量或时长限制的产品等篡改订单参数问题；如上传文件时应对文件类型前后端都做白名单校验，并通过随机数重命名文件名和文件路径，且将保存文件的文件夹权限设置为不可执行；

b) 业务逻辑设计的完整性，逻辑设计不得存在可绕过必要前置操作，进行后续操作。如通过手机验证码找回密码的业务流程中，可通过篡改应答报文的方式跳过验证码验证，直接设置新密码，或通过未授权的 URL 直接跳转到设置新密码的页面；

c) 验证功能，涉及短信验证码、图形验证码的功能，应设计验证码一次有效及验证码有效期，避免短信轰炸、验证码复用等问题；

d) 会话状态的更新，用户退出业务系统后应将会话同步置为失效，如无需长时间保持会话的业务系统，需设置会话失效时间；

e) 用户验证失败后的提示、找回等功能，登录业务应对有效账户和无效账户身份验证失败时返回的信息进行模糊化处理，应具备防爆破措施，认证鉴权要求同用户认证章节中的要求。用户注册、密码找回业务可以根据业务需求返回最小必需提示信息，但应设置同一用户用户名枚举次数及密码错误次数限制策略；

f) SQL 注入漏洞的防护，禁止在代码中使用 SQL 拼接或等效于拼接的方式构造 SQL 语句，应使用参数绑定的方式构造动态 SQL 语句，或对 SQL 语句在后端进行预处理，避免 SQL 注入的潜在安全问题。

6.10.1.6 API 安全

API安全模块通过请求认证与鉴权、数据加密、实时监控、禁用异常调用等手段保障用户及服务平台系统的安全。API安全模块应支持以下功能：

a) API 请求认证与鉴权

1) API 接口访问源白名单、黑名单配置能力，可拒绝白名单外、黑名单内来源的请求。原则上，仅允许请求方需使用特定的 IP、端口发起 API 访问。
2) API 接口对调用方进行权限划分与管理，如调用源按管理员（分配账号）、操作员（具体操作）、审计员（查看审计日志）角色进行分配时，需遵从三权分立，不能交叉。
3) API 接口对调用方进行认证，防止未授权访问、越权访问、遍历访问。
4) 使用 Token 等机制进行授权管理，所有的授权需要有合理的过期时间。
5) API 接口鉴别伪造请求的能力。
6) API 相关密钥（如 API Key）的保护，不允许保存在 API 请求端代码内（如直接嵌入页面 JS 代码或注释内等）。
7) 涉敏接口限制调用频率，具备认证失败锁定策略，如网关根据请求 IP 限制其指定时间内调用次数。

b) API 数据请求

1) 对客户端请求中涉及的敏感信息参数采用 POST 方式，且需要加入随机产生的 Token 参数进行校验。
2) 对前端输入的非正常参数（如 script\select\and\or 等特殊字符、系统命令或恶意代码）进行后端过滤，杜绝绕过 API 直接对数据库进行操作。
3) 对请求中携带的违法有害信息进行监测并过滤。

c) API 数据返回

1) 对后端输出展现内容进行转义处理。
2) 返回状态时使用统一的不泄露内部敏感信息的提示语。
3) 返回敏感数据（包括不限于姓名、身份证号、电话号码、邮箱地址、地址、账号口令）时，对敏感数据进行加密。

4） API 对反馈内容进行违法有害信息监测，可阻断违法有害信息返回。

d） 传输信道要求

对暴露在互联网的产品和系统使用 HTTPS 协议进行传输。

e） API 审计日志

1） API 操作日志审计能力，记录操作审计日志。记录内容要求：发生日期时间、用户名、事件类型、事件详情（如操作内容，是否成功）。

2） 对涉及大量数据流通交互的 API 配置针对数据操作与流动的监控功能，流动日志主要记录内容包括：发生日期时间、数据对接方/用户名、数据流通频次、事件类型、事件详情（如对接了多少数据量）等。

3） 日志保存时长不小于 6 个月。

f） API 禁用能力

1） 禁止异常的 API 请求源对 API 进行调用。

2） API 服务接口本身的禁用功能。

6.10.1.7 日志留存

日志留存模块通过记录系统的运行状态和操作历史帮助技术人员快速定位故障，恢复服务，同时帮助服务平台满足各种安全法规和合规性要求。日志留存模块应支持以下功能：

a） 对用户权限变更、数据授权访问、数据批量复制、数据修改、数据销毁、数据接口调用、任务调度、测量时间序列、态重置频率等重点环节实施日志留存管理，日志记录信息应包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等，并确保日志记录完整、准确，以供查阅和审计，日志留存时间不少于 6 个月；

b） 基于用户审计需求的可追溯性日志导出功能，记录量子任务的上传、编译、调度、执行全过程。

6.10.1.8 业务系统加固

业务系统加固模块通过漏洞扫描、渗透测试、口令设置等手段保障用户和服务平台系统的安全。业务系统加固模块应支持以下功能：

a） 漏洞扫描、渗透测试功能，业务系统包括中间件不得存在中危及以上漏洞。

b） 对业务系统中使用的各组件、中间件的口令的提前规划，禁止使用空口令、默认口令、弱口令、通用口令、长期不变口令、大量不同设备（系统）使用相同口令等，禁止密码明文保存。

6.10.2 主机安全功能

6.10.2.1 量子计算机安全

量子计算机安全模块通过对量子计算硬件资源和外围保障系统的工作状态进行监控保障量子计算机的运行安全。量子计算机安全模块应支持以下功能：

a） 对量子计算机硬件资源的工作状态和使用情况进行监控，监控项目要求如表 1 所示；

b） 对用户提交的量子计算任务进行参数限制，包括但不限于对用户提交的量子线路深度和宽度或量子模拟任务演化时长的限制，单次采样的时长不应当超过各技术路线合理的相干时间；

c） 对用户提交的量子计算任务进行安全校验和沙箱分析，防止恶意构造的量子电路或量子计算任务造成硬件资源耗尽、系统崩溃或侧信道泄露；

d） 对量子计算机外围保障系统的工作状态进行监控，包括但不限于电源工作状态、温度等。

表1　量子计算机硬件资源的监控要求

监控项目	用户	服务平台提供商
提供量子计算资源占用情况的监控	必选	必选
提供服务进程的监控	必选	必选
定期获取量子计算机整体运行状态，包括但不限于单比特门保真度、双比特门保真度、读取保真度、能量弛豫时间 T1、相位弛豫时间 T2 等	可选	必选
提供量子计算机电源工作状态的监控	可选	必选
提供量子计算机测控系统 CPU、内存、硬盘等工作状态和性能情况的监控	可选	必选
提供量子计算机硬件和经典硬件互联网络工作状态、网络流量情况的监控	可选	必选
提供事件的监控	可选	必选
提供任务队列的监控	可选	必选

6.10.2.2　经典服务器安全

经典服务器安全模块通过对经典服务器进行实时监控、设置防火墙、设置访问权限等操作保障经典服务器的运行安全。经典服务器安全模块应支持以下功能：

a）　对重要经典服务器的 CPU、硬盘、内存、网络等资源的工作状态和使用情况进行监控，监控项目要求应满足 GB/T 37736-2019 中 7 的规定；

b）　对经典服务器部署安全防护措施，如主机防火墙、主机 IDS 等。

c）　对操作系统和数据库系统访问控制配置，对登录用户进行身份标识和鉴别，并设置密码策略、账户策略、审核策略、用户权限等安全策略；

d）　对计算节点、存储节点、管理节点中的各类经典服务器和数据库等设备进行安全评估优化，必要时实施安全加固；

e）　应用统一的策略对经典服务器操作系统软件、应用软件等进行升级。

6.10.2.3　网络安全

网络安全模块通过对网络划分安全域、设置用户访问权限、设置防火墙等手段保障网络运行安全。网络安全模块应支持以下功能：

a）　根据所部署应用的用户访问特性和核心功能，将服务平台网络从总体上划分为多个不同的功能区和安全域，如公共区、受限区和核心区等；

b）　在网络和系统层面划分安全域，将业务系统、安全技术有机结合，形成完整的防护体系，对同一安全域内的系统进行统一规范的保护，同时限制系统风险在网内的任意扩散；

c）　网络安全边界，满足服务平台网络不同功能区域之间相互安全通讯的需求；

d）　VPN 远程接入服务，确保公网上传输的私有数据安全，并实现对接入用户的认证；

e）　在网络出口处部署防火墙，并依据业务需求设置合理的访问控制措施；

f）　流量清洗设备，监控、告警、防护对服务平台的应用服务器发起的 DoS/DDoS 攻击。

6.10.2.4　虚拟化环境安全

虚拟化环境安全模块通过对虚拟化服务器、虚拟化网络、虚拟化存储进行安全加固保障服务平台虚拟化环境的运行安全。虚拟化环境安全模块应支持以下功能：

a）　服务器虚拟化安全

1） 虚拟机管理接口应严格限定为管理虚拟机所需的接口，并关闭无关的协议端口；
2） 内核模块应通过虚拟化设备提供商的认证；
3） 设置单一虚拟机的资源限制量，保护虚拟机的性能不因其他虚拟机尝试消耗共享硬件上的太多资源而降低；
4） 通过隔离措施实现虚拟机资源间的安全隔离，如 CPU 调度隔离、内部网络隔离、不同虚拟机的内存隔离、不同虚拟机的存储隔离等，并只允许符合安全策略的虚拟机之间实现互相访问；
5） 管理员客户自定义虚拟机之间的安全策略。

b） 网络虚拟化安全
1） 基于虚拟机安全组实现虚拟网络的逻辑隔离，提高网络安全性；
2） 支持通过 SDN 或虚拟防火墙等方式为不同用户设置独立、可定制的安全策略功能；
3） 提供分权限、分角色的管理配置能力，确保不同租户可独立管理自身资源的安全策略、用户认证信息等；
4） 支持 IPsec VPN 等加密通信功能、支持抗 DoS 攻击的功能；
5） 硬件防火墙应能支持不少于 200 个虚拟防火墙；
6） 虚拟化平台提供逻辑分区的边界防护能力，支持网络分段与安全策略的集中管理。

c） 存储虚拟化安全
1） 集中化的客户密钥管理与分发机制，实现对客户信息存储的高效安全管理与维护；
2） 客户数据在上传、存储前的自行加密功能。

6.10.3 Web 安全功能

6.10.3.1 垂直越权漏洞防护

垂直越权漏洞是指低权限用户能够访问或执行高权限用户的功能或数据，这种漏洞可能导致平台的安全性受到威胁。服务平台垂直越权漏洞防护应支持以下功能：

a） 用户权限管理功能，使用户只能访问已授权的功能和数据，禁止低权限用户访问高权限用户的功能和数据；
b） 输入验证和过滤功能，对用户输入的数据进行严格的验证和过滤，防止恶意用户利用漏洞进行攻击；
c） 会话管理功能，确保会话令牌的安全性和随机性，防止会话劫持等攻击；
d） 漏洞扫描与修复功能：定期进行漏洞扫描和修复，及时发现和处理异常行为和安全事件，确保平台不存在垂直越权漏洞。

6.10.3.2 跨站脚本攻击防护

跨站脚本攻击防护应支持以下功能：

a） 输入验证和过滤功能，对用户输入的数据进行严格的验证和过滤，防止恶意脚本的注入；
b） 输出编码和转义功能，在将数据显示在网页上时，对特殊字符进行编码和转义，防止恶意脚本的执行；
c） 内容安全策略功能，使用内容安全策略（CSP）等技术，限制网页中可执行脚本的来源，防止恶意脚本的加载和执行；
d） 漏洞扫描与修复功能：定期进行漏洞扫描和修复，及时发现和处理异常行为和安全事件，确保平台不存在跨站脚本攻击。

注：跨站脚本攻击（XSS）是一种常见的Web安全漏洞，攻击者通过在Web页面中插入恶意脚本，使其在用户浏览器中执行，从而窃取用户信息、篡改网页内容等。

6.10.3.3 SQL 注入漏洞防护

SQL注入漏洞指攻击者利用服务平台应用程序中的 SQL 注入漏洞，通过构造恶意的 SQL 语句，获取或篡改数据库中的敏感信息，从而危害服务平台的安全。SQL注入漏洞防护应支持以下功能：

a) 对用户输入的数据进行严格的验证和过滤功能，防止攻击者注入恶意的 SQL 语句；
b) 使用参数化查询或预编译语句功能，避免直接拼接 SQL 语句，减少 SQL 注入的风险；
c) 限制数据库用户的权限功能，确保只有必要的用户才能访问数据库，并限制其操作权限；
d) 漏洞扫描与修复功能：定期进行漏洞扫描和修复，及时发现和处理异常行为和安全事件，确保平台不存在 SQL 注入漏洞。

6.10.3.4 平行越权漏洞防护

平行越权漏洞是指在一个服务平台上，一个用户或应用程序能够执行其他同级用户或应用程序的操作，从而获取不应有的权限或访问不应访问的数据。这种漏洞可能会导致数据泄露、系统被攻击等安全问题。平行越权漏洞防护应支持以下功能：

a) 权限校验功能，在服务平台的应用程序中，对于每一个需要进行数据操作的请求，都应该进行权限校验；
b) 数据加密功能，对于敏感数据，应该使用加密技术来保护其安全性，防止未经授权的用户访问或篡改数据；
c) 访问控制功能，实现严格的访问控制策略以限制用户的访问权限。例如，可以限制用户的 IP 地址、使用时间段等，以减少未经授权的访问；
d) 漏洞扫描与修复功能：定期进行漏洞扫描和修复，及时发现和处理异常行为和安全事件，确保平台不存在平行越权漏洞。

6.10.3.5 跨站请求伪造漏洞防护

跨站请求伪造漏洞防护应支持以下功能：

a) CSRF 令牌功能，在表单中添加唯一的 CSRF 令牌，确保表单提交的数据是合法的；
b) HTTP Referer 字段验证功能，验证请求中的 Referer 字段，确保请求来源于受信任的网站；
c) SameSite Cookie 属性功能，设置 Cookie 的 SameSite 属性，限制 Cookie 在跨站请求中的使用；
d) 限制敏感操作权限功能，对于涉及敏感操作的请求，可使用二次确认或者输入密码等方式，确保用户的操作是合法的；
e) 漏洞扫描与修复功能：定期进行漏洞扫描和修复，及时发现和处理异常行为和安全事件，确保平台不存在跨站请求伪造漏洞。

注：跨站请求伪造（Cross-Site Request Forgery，CSRF）漏洞是指攻击者利用用户在已登录状态下的身份，伪造合法请求对服务平台进行恶意操作的安全漏洞。这种漏洞可能会导致用户在不知情的情况下执行恶意操作，从而危害服务平台的安全。

附 录 A
（资料性）
量子计算服务平台的服务模式概述

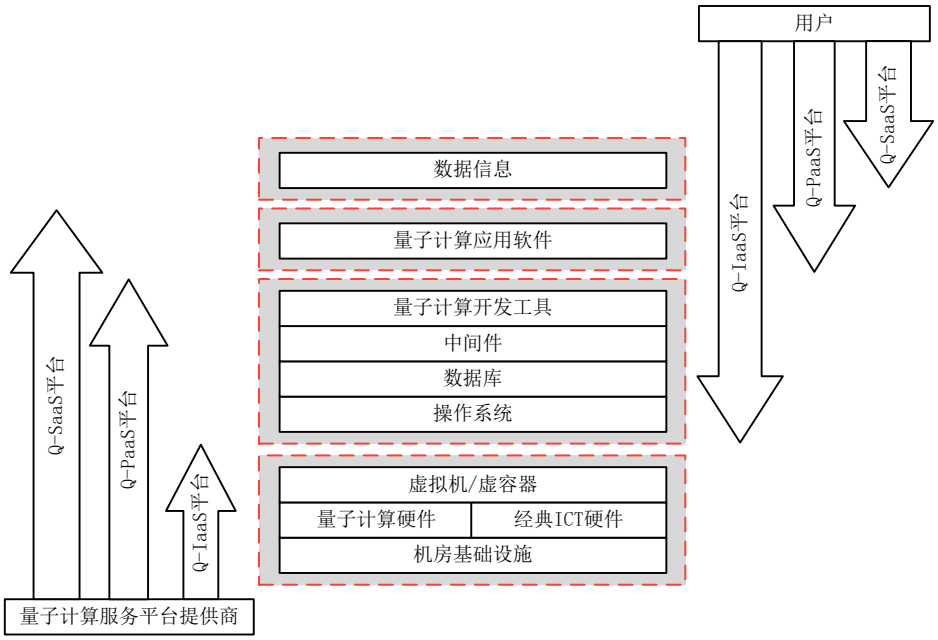
量子计算服务平台的服务模式包括以下类型：

a) 量子基础设施即服务（Q-IaaS）：提供量子计算机的硬件及配套设施，供用户访问和调用平台上的资源。包括量子计算机（包括门型量子计算机或非门型量子计算机）、量子资源经典模拟器、经典计算资源、存储资源等，用户无需维护底层硬件，实现低成本的底层开发和科学研究等活动。

b) 量子平台即服务（Q-PaaS）：提供由量子计算相关基础设施和中间件组成的开发平台，支持量子计算软件开发。用户可使用量子计算软件开发平台，开发量子软件和量子算法库，并通过平台连接到不同厂商的量子计算硬件进行计算，支持单一平台或跨平台兼容开发，可进行经典—量子混合计算，并自动分配经典计算资源和量子计算资源。

c) 量子软件即服务（Q-SaaS）：面向特定行业应用和需求，提供已封装的量子计算应用服务方案。用户可依靠量子计算软硬件资源解决特定的实际问题，无需全面掌握量子计算知识和编程技能。

三种服务模式下，服务平台提供商与用户的管理域差异如图A.1所示。



图A.1 三种服务模式的量子计算服务平台示意图

附 录 B
（资料性）
量子计算服务订单质疑和售后功能概述

由于量子计算机存在一定不稳定性，量子计算机性能和结算结果受环境影响大，因此可能导致计算结果出现明显偏差。为保障用户权益，可参考下述量子计算服务订单质疑和售后处理的流程和规范。

B.2 量子计算性能校验流程

性能校验流程目的：为确保量子计算服务平台提供的量子计算服务性能可靠，增加量子计算性能校准流程，确保量子计算机在校验后提供的校验服务是正常的，进而避免用户对计算结果的质疑。

性能校验在量子计算服务流程中的位置：对于门型量子计算机，该流程需放置在用户任务执行任务前，此处任务指单一用户连续提交的任务集。其中校验间隔（绝对时间间隔）可由服务平台供应商根据硬件性能确定。如单一量子计算机在给不同用户执行任务时，应在切换用户时为下一个用户提供校验服务。对于非门型量子计算机，可在任务计算前执行校验、任务计算中同步校验或者根据硬件性能定期执行校验等。

该性能校验旨在对量子计算机性能进行验证该校验结果作为后续可能出现售后问题的依据。

门型量子计算机性能校验流程：

a) 校验线路生成：（1）校验线路的量子比特数目：量子比特数目尽可能与用户订单所要求的比特数目保持一致，如客户提供的比特数目超过服务平台中量子资源经典模拟器的模拟能力，则将模拟器中的固定上限比特数目作为校验线路的比特数目。（2）校验线路生成：考虑到量子资源经典模拟器的性能和执行效率，可采用随机生成的 Clifford 线路作为校验线路，并通过量子资源经典模拟器进行全振幅模拟。（3）校验中测量集选取：校验任务中应随机选择一类（或单个）Pauli 测量作为量子线路最终测量集，量子计算机通过多次测量得到测量量子态的概率分布结果；量子资源经典模拟器则可以根据全振幅模拟得到对应的理想结果。
b) 采样与对比：通过运行上述校验线路，对测量结果和概率分布进行分析，将量子计算机给出的结果和经典模拟器结果进行对比，计算量子计算机当前的保真度和置信值。
c) 结果记录与应用：记录结果，如果保真度和置信值均大于设定的阈值则说明量子计算机当前处于可信服务状态。

非可信服务状态任务处理：若任务执行期间量子计算机硬件处于非可信服务状态，可继续执行，但要保留客户售后的权利。

非门型量子计算机性能校验流程：

a) 校验基准建立：选取有代表性的基准问题，如最大割问题等，或依据应用场景选取合适的基准问题。根据问题模型，生成基准测试任务，并用经典算法计算参考解作为对比标准；
b) 执行基准测试与评估：将基准测试任务输入量子计算机并执行多次计算，将量子计算机结果与经典参考解进行对比分析，输出判定可信服务状态的关键指标数据；
c) 记录结果与应用：记录测试与评估过程的所有数据，如果可信服务状态指标优于设定阈值，则说明量子计算机当前处于可信服务状态。

非可信服务状态任务处理 ：若任务执行期间量子计算机硬件处于非可信服务状态，可暂停服务并对量子计算机进行调试，直到恢复到可信服务状态；或继续进行服务，但要保留客户售后的权利。

B.3 售后处理

若用户发现计算结果存在明显偏差,且经确定是由于量子计算机性能问题导致的,用户可申请售后。售后处理将依据量子逻辑门操作校准流程所记录的性能状态等信息，安排在机器性能稳定时重新运行相关订单任务。

（资料性）
数据保存功能

C.1 概述

量子计算作为一种新型的计算范式，计算过程涉及到的数据量很大，且数据类型的种类复杂，包括经典数据和量子相关数据。对于门型量子计算机，数据的数据类型、线路编译的信息、中间态数据、量子计算后结果数据、输出数据以及部分非核心结果等。对于非门型量子计算机，数据类型包含经典控制参数、量子态信息等，从数据产生角度可分为原始输入数据、量子系统演化过程中的中间数据、最终输出结果数据等。保存中间态和部分非核心结果等。因此，在利用量子计算机提供量子云平台服务的时候，需要对数据进行分类保存，合理规划量子信息与经典数据的转换和保存方式，包括考虑将哪些量子信息转换为对应的经典数据进行存储。

C.2 量子计算服务平台数据保存级别

对于门型量子计算机：

考虑到量子云计算业务和数据存储的复杂性，以及数据存储量的需求，现将量子云计算服务的数据存储分成如下几个级别（从level-1到level-4，数据存储要求更高，将更多支撑性数据进行存储）：

Level-1：只保存用户任务代码或编译后的量子线路（包含线路和门结构，以及含参门的参数信息），和最后期望值结果或者程序中要求给出的最终计算结果（通常为一个数值式结果）。

Level-2：在level-1的基础上，保存最终量子态探测的结果（包含每个shot、repeat后的测量结果，包含所有物理比特，即计算比特和ancilla），存储数据类型为量子态的概率分布

Level-3：在level-1和2的基础上，保存了每一次具体实现线路的相关参数，包括含参门信息，当前环境参数信息，校准的参量信息等（因为量子计算机一般都是随时间环境变化很大的，所以需要记录每一次时间的环境参数，频率等校准参数也是要保留的）

Level-4：在level-1~level-3的基础上，考虑到未来量子纠错和in-circuit探测的需求，还需要保存其相关中间量子态测量的结果和反馈指令，逻辑编码、解码的过程和结果。

对于非门型量子计算机：

考虑到量子云计算业务和数据存储的复杂性，以及数据存储量的需求，现将量子云计算服务的数据存储分成如下几个级别（从level-1到level-3，数据存储要求更高，将更多支撑性数据进行存储）：

Level-1：仅保存用户输入的原始输入数据，以及最终计算得出的能量基态或低能态结果（通常为数值形式，代表系统最低能量状态对应的参数值）。此级别满足用户获取核心计算结果的基本需求。

Level-2：在 level-1 基础上，保存每次独立计算采样最终量子态测量的详细结果，覆盖所有参与计算的量子比特信息。这些数据为用户提供更丰富的计算后信息，便于分析系统最终状态统计特性与量子比特相位变化规律等。

Level-3：在 level-1 和 level-2 的基础上，保存每次独立计算采样所有中间量子态数据，并记录每一个任务中每次独立计算采样计算过程的关键参数，包括量子系统初始状态参数、运行时环境参数、设备校准参数以及每次独立计算采样过程中的关键中间参数等。这些参数助力用户深度剖析计算过程，完整复现计算场景，精准排查误差来源，高效优化模型参数设置。

C.3 数据存储时长

当用户利用量子云平台进行计算任务处理时，可以根据如上类别进行数据的存储，考虑到不同level的数据重要性不一样，其数据保存时间长短也不一样。因此可以根据保存时间长短，进行评判和要求。此处存储时长指的是，在数据存储时长内，数据进行硬件存储后，用户可以随时将对应经典数据提取出来转移至用户端。

（资料性）
量子计算逻辑门的完备性

D.1 概述

若一组量子门的组合能以任意精度逼近任意单量子比特酉变换和任意两量子比特酉变换（对多量子比特系统，两量子比特门是实现纠缠的关键），则称这组门是通用的（Universal），即具备完备性。

数学表述：对于任意酉矩阵$U\in U(2^n)$（n 为量子比特数），存在由基本门组成的序列 $G_k\cdots G_2G_1$，使得$\|U-G_k\cdots G_2G_1\|<\varepsilon$ （ ε 为任意小的正数）。

D.2 常见的量子计算逻辑门完备集

以下是几类被证明具有完备性的量子门组合：

D.2.1 单比特门+两比特受控非门（CNOT门）

单比特门：如泡利门（X, Y, Z）、哈达玛门（H）、相位门（S）等，可实现单量子比特的任意旋转。

两比特受控非门（CNOT门）：CNOT门是实现两量子比特纠缠的基本门，其矩阵表示见公式（D.1）：

$$\mathrm{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \quad \text{(D.1)}$$

D.2.2 哈达玛门（H门）+T门+CNOT门

哈达玛门（H门）：常用于产生叠加态，其矩阵表示见公式（D.2）：

$$\mathrm{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix} \quad \text{(D.2)}$$

T 门：相位门的一种，其矩阵表示见公式（D.3），其作用是引入 $\pi/4$的相位差：

$$\mathrm{T}=\begin{pmatrix}1&0\\0&e^{i\pi/4}\end{pmatrix} \quad \text{(D.3)}$$

D.2.3 其他完备集

单比特门+任意两量子比特纠缠门：例如使用控制相位门（CPHASE）替代 CNOT 门，只要两量子比特门能生成足够的纠缠，即可与单比特门组合成完备集。

多量子比特门：在某些量子计算模型（如拓扑量子计算）中，可能使用三量子比特门作为基本单元，但核心仍是通过组合实现任意酉变换。

D.3 完备性的数学证明思路

D.3.1 群论基础

量子门的酉变换对应于酉群 $U(d)$（d 为希尔伯特空间维度，$d=2^n$）的元素。完备性问题转化为：基本门集合生成的子群是否在 $U(d)$中拓扑稠密（即任意元素可由子群元素逼近）。

D.3.2 关键定理

Solovay-Kitaev 定理：指出在$SU(d)$ 中，任何有限生成的稠密子群都可以在多项式时间内逼近任意元素，误差随门数指数下降。这为量子门的通用性提供了理论保证。

两量子比特门的作用：单比特门生成$SU(2)$，两比特门（如 CNOT）可将$SU(2)$ 的作用 “扩展”到整个多量子比特空间，从而生成 $SU(2^n)$。