ICS 35.100.05
CCS L 80

T/ZGCMCA

中 国 移 动 通 信 联 合 会 团 体 标 准

T/ZGCMCA 026-2025

元宇宙资产库跨链互操作技术规范

Technical Specification of Cross-Chain Interoperability for Metaverse Resource Library

2026 - 1 - 13 发布　　2026 - 01 - 25 实施

中国移动通信联合会　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。

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这些专利的责任。

本文件由中国移动通信联合会提出并归口。

本文件起草单位：咪咕新空文化科技（厦门）有限公司、清华大学、北京邮电大学、中国国家博物馆、十一维度（厦门）网络科技有限公司、北京力群芬芳文化发展有限公司、中国科学院上海微系统与信息技术研究所、北京微视威信息科技有限公司、中国联合网络通信有限公司、中兴通讯股份有限公司、福建百宝图科技有限公司、浙江大学、光线云（杭州）科技有限公司、共生生（厦门）科技有限公司、北京兴云数科技术有限公司、超元纬度（北京）科技有限公司、北京工业大学、中国移动通信联合会区块链与数据要素专业委员会。

本文件主要起草人：张小磊、杨定康、张松海、乔秀全、李华飙、余海箭、黄琪雯、史雪振、高岩、盖孟、马睿智、江洪峰、于涛、王玉旺、张贺、咸国坤、万远亮、吴伯海、王锐、吴勇、叶帅、于正勇、黄莹晶、郭雨晨、郭宏蕾、温正棋、赵鑫、何伟、陈晓华。

本文件首次发布。

元宇宙资产库跨链互操作技术规范

1 范围

本文件规定了元宇宙资产库跨链互操作的术语和定义、总体架构、技术要求、安全要求、性能要求、测试方法。

本文件适用于元宇宙平台、区块链服务提供商、数字资产交易平台等相关机构，用于指导元宇宙资产库跨链互操作的系统设计、开发、部署和运营。

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 35299-2017 信息安全技术 区块链 参考架构

GB/T 36344-2018 信息技术—数据质量评价指标

GB/T 37988-2019 信息安全技术—数据安全能力成熟度模型

GB/T 42752-2023 区块链和分布式记账技术参考架构

3 术语和定义

GB/T 36344-2018界定的及以下术语和定义适用于本文件。

3.1

元宇宙 metaverse

由完整稳定运行的技术，内容、经济、协作和治理子系统构成的，具有高度沉浸、实时永续，自主创造、开放互联等特征的，虚拟与现实融合交互的新型社会生态系统。

3.2

数字资产 digital Asset

以数字形式存在的、具有经济价值和可交易性的资产，包括虚拟货币、NFT（非同质化代币）、数字艺术品、虚拟土地等，其权属和交易记录存储在区块链等分布式账本上。

3.3

分布式账本 distributed ledger

在分布式节点间共享并使用共识机制实现具备一性的账本。

3.4

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

3.5

跨链互操作 cross-chain interoperability

不同区块链网络之间实现数据交换、资产转移、智能合约调用等交互操作的能力，以打破区块链之间的孤岛效应，促进元宇宙资产的流通和应用。

4 缩略语

下列缩略语适用于本文件：
NFT：非同质化代币（Non-Fungible Token）
HTLC：哈希时间锁定合约（Hashed Timelock Contract）
VPN：虚拟专用网络（Virtual Private Network）
DDoS：分布式阻断服务（Distributed Denial of Service attack）

5 总体要求

5.1 目标

实现元宇宙资产库在不同区块链平台间的无缝连接和协同工作，支持跨链资源的查询、调用、转移等操作，为元宇宙应用提供统一、高效的数据交互基础，促进元宇宙生态的繁荣与发展。

5.2 原则

5.2.1 兼容性

跨链技术应兼容不同类型的区块链系统（如公有链、联盟链、私有链），以及不同的共识机制（如工作量证明、权益证明、实用拜占庭容错等）。

5.2.2 安全性

应采用加密技术、身份认证机制和安全审计措施，保障跨链数据传输和资源交互过程中的数据安全、隐私保护和操作可追溯。

5.2.3 高效性

优化跨链交互流程和通信协议，减少数据传输延迟和处理时间，提高跨链操作的响应速度和吞吐量，满足元宇宙应用对实时性和高并发的需求。

5.2.4 可扩展性

设计灵活的技术架构，便于新增区块链系统接入元宇宙资产库跨链网络，支持系统功能和性能的扩展，以适应元宇宙生态不断发展的需求。

5.2.5 标准化

遵循统一的技术标准和规范，确保不同开发者和机构构建的元宇宙资产库跨链系统具有互操作性和兼容性，降低系统集成和对接成本。

5.3 应用场景

5.3.1 虚拟资产跨平台流通

用户在不同元宇宙平台上的虚拟资产（如虚拟货币、数字藏品、游戏道具等）可通过跨链技术在多个区块链上的元宇宙资产库之间进行转移和交易，实现资产的跨平台流通和价值互通。

5.3.2 场景数据共享

不同元宇宙应用场景中的场景数据（如虚拟环境地图、建筑模型、物理规则等）可通过跨链技术在元宇宙资产库间共享，支持多平台联合开发和场景融合，丰富用户体验。

5.3.3 用户身份统一管理

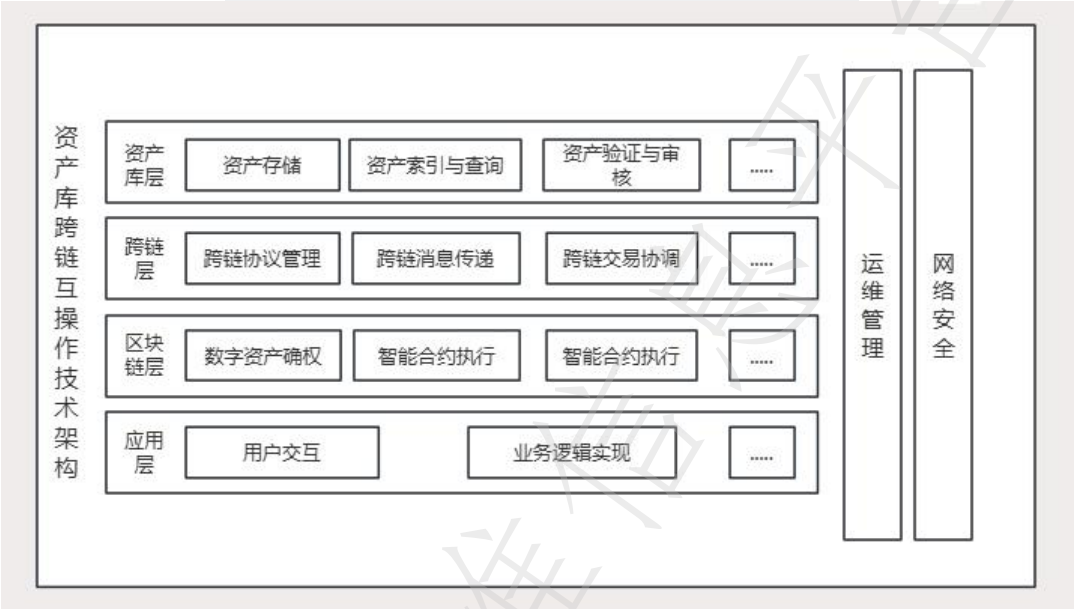
用户在不同元宇宙平台的身份信息存储在元宇宙资产库中，通过跨链技术实现身份认证和权限管理的互通，使用户能够以统一身份访问多个元宇宙应用，提升用户体验和管理效率。

6 技术架构

6.1 总体架构

元宇宙资产库跨链互操作技术架构应包含资产层、区块链层、跨链层、应用层，各层之间相互协作，实现元宇宙资产的跨链流通与交互，架构示意见图1。

图1 元宇宙资产库跨链互操作技术架构示意图



6.2 资产库层

6.2.1 功能

6.2.1.1 资产存储

负责存储数字资产的详细信息，包括元数据（如数字艺术品的作者、创作时间、描述等）、资产所有权信息（记录资产所属用户的 DID 等）以及资产的历史交易记录等。

6.2.1.2 资产索引与查询

具备高效的索引机制，能够快速查询和检索资产库中的数字资产。支持根据资产类型、所有者、交易时间等多种维度进行查询。

6.2.1.3 资产验证与审核

对进入资产库的数字资产进行验证和审核，确保资产的真实性、合法性和合规性。

6.2.2 技术要求

6.2.2.1 存储

应采用分布式存储技术，结合关系型数据库（如 MySQL）和非关系型数据库（如 MongoDB），对结构化和非结构化的资产数据进行有效管理，资产数据不依赖于任何第三方平台进行渲染应用，在不与平台关联的情况下也能够独立运行。同时，遵循GB/T 37988-2019的规定。

6.2.2.2 索引

索引设计应满足以下要求：

a) 对于经常作为查询条件的字段，包括资产 ID、交易发起方和接收方标识等，应建立相应的索引。在多表连接查询时，连接字段也应创建索引，并且保证字段在不同表中的类型一致；

b) 索引应与主数据保持一致，当跨链交易数据发生更新、删除等操作时，索引也应及时进行相应的更新；

c) 应采用分布式存储和管理方式，确保在不同的区块链节点或存储节点上都能快速访问和更新索引信息；
d) 应支持语义索引，即根据数据的语义信息进行索引构建。

6.3 跨链层

6.3.1 功能

6.3.1.1 跨链协议管理

支持多种跨链协议，包括哈希时间锁合约（HTLC）、跨链桥协议（如基于侧链的跨链桥、中继链跨链桥等），根据不同的跨链需求选择合适的协议进行资产跨链转移和数据交互。

6.3.1.2 跨链消息传递

负责在不同区块链网络之间传递跨链交易消息和相关指令，对消息进行加密、签名和验证，防止消息被篡改和伪造。

6.3.1.3 跨链交易协调

协调源链和目标链上的跨链交易执行，确保交易在不同链上的状态一致性。

6.3.2 技术要求

6.3.2.1 协议兼容性

跨链层应能够兼容不同区块链网络的共识机制、智能合约标准和数据格式。对于采用不同共识算法（如 PoW、PoS、DPoS 等）的区块链，通过适配层进行转换和协调，确保跨链操作的顺利进行。应支持多种智能合约标准，包括以太坊的 ERC-721、ERC-1155 等，以及其他区块链平台的类似标准，实现数字资产在不同链上的互认和交互。同时，还应满足 GB/T 42752-2023的要求。

6.3.2.2 消息传递机制

采用 RabbitMQ、Kafka 等消息队列技术，进行跨链消息的异步传递。设置消息重试机制和超时处理机制，确保消息在网络不稳定等情况下也能成功传递。同时，运用加密技术（如 AES 加密算法）对消息内容进行加密，使用数字签名技术（如椭圆曲线数字签名算法 ECDSA）对消息发送方进行身份验证，保证消息的安全性和完整性。

6.4 区块链层

6.4.1 功能

6.4.1.1 数字资产确权

利用区块链的不可篡改和可追溯特性，对数字资产进行确权登记，确保资产的所有权明确且唯一，同时还可采用国家版权中心进行登记，将数字资产的唯一权益进行三权分置，包括持有权、经营权和使用权。通过智能合约实现资产持有权、经营权和使用权的转移和变更记录，为资产的交易和流转提供可信的基础。

6.4.1.2 智能合约执行

支持在区块链上部署和执行智能合约，实现数字资产的自动化交易、收益分配、版权管理等功能。

6.4.1.3 共识与验证

各区块链节点通过共识机制（如工作量证明、权益证明等）对交易进行验证和确认，确保区块链账本的一致性和可靠性。在跨链操作中，参与跨链的区块链节点需要协同工作，对跨链交易进行联合验证，保证跨链交易的合法性和安全性。

6.4.2 技术要求

6.4.2.1 区块链平台选择

应根据应用场景的不同，选择区块链平台（如以太坊、Solana 、Polkadot、Cosmos 等）。同时，也可根据实际情况搭建联盟链或私有链，满足特定组织或行业的需求。

6.4.2.2 智能合约安全

应加强智能合约的安全审计和漏洞检测，在智能合约部署前，采用专业的安全审计工具（如 MythX、Slither 等）对合约代码进行全面检查，发现并修复潜在的安全漏洞，定期对已部署的智能合约进行安全评估和更新，确保智能合约在运行过程中的安全性。

6.5 应用层

6.5.1 功能

6.5.1.1 用户交互

为用户提供友好的界面，实现用户与元宇宙资产库和跨链互操作功能的交互。包括资产的查询、购买、出售、跨链转移等操作，以及用户身份管理、钱包管理等功能。

6.5.1.2 业务逻辑实现

根据元宇宙应用的具体业务需求，实现相应的业务逻辑。包括在元宇宙游戏中，实现虚拟道具的跨链使用和交易；在数字艺术展览中，实现数字艺术品的跨链展示和销售等功能。

6.5.2 技术要求

6.5.2.1 界面设计

采用响应式设计，确保应用界面在不同设备（如电脑、手机、平板等）上都能友好显示和操作。注重用户体验，简化操作流程，提供清晰的提示和反馈信息，使用户能够方便快捷地进行各种操作。

6.5.2.2 业务逻辑开发

运用合适的编程语言和开发框架，根据业务需求进行高效、可靠的业务逻辑开发。遵循软件工程的最佳实践，对代码进行良好的组织和管理，提高代码的可维护性和可扩展性。同时，确保应用层与资产库层、跨链层和区块链层之间的接口调用稳定、准确。

7 技术要求

7.1 资产表示与编码

7.1.1 数字资产标准化

7.1.1.1 数字资产应遵循标准化的表示方法，确保在不同区块链网络和元宇宙平台之间的互认和流通。对于 NFT 资产，应符合主流的 NFT 标准（如以太坊的 ERC-721、ERC-1155 标准）或其他区块链平台认可的等效标准。

7.1.1.2 资产的元数据应按照统一的格式进行描述，包括但不限于资产名称、唯一标识符、资产类型、创作者信息、创作时间、资产描述、资产图片或链接等。

7.1.2 资产编码格式

7.1.2.1 应采用通用的资产编码格式，包括 JSON（JavaScript Object Notation）或 CBOR（Concise Binary Object Representation），在通过 DOM 格式对数字资产进行编码。编码后的资产数据应保障在互联网传播时的数据加密性、可控性，同时应能够准确、完整地表达资产的所有信息，包括资产的属性、所有权关系和交易历史等。

7.1.2.2 在跨链传输过程中，应确保资产编码格式的兼容性，避免因编码格式不一致导致资产信息丢失或错误。

7.2 跨链通信协议

7.2.1 协议选择与适配

7.2.1.1 应支持多种跨链通信协议，包括哈希时间锁合约（HTLC）、跨链桥协议（包括基于侧链的跨链桥、中继链跨链桥等）以及新兴的跨链互操作性协议（如 Cosmos 的 IBC 协议、Polkadot 的 XCM 协议等）。根据不同的跨链场景和需求，选择合适的跨链通信协议，并进行必要的适配和优化。

7.2.1.2 在选择跨链协议时，应综合考虑协议的安全性、性能、兼容性和可扩展性等因素。对于小额、高频的数字资产跨链交易，宜选择哈希时间锁合约，具有简单、高效的特点；而对于大规模、复杂的跨链资产转移和交互，宜选择跨链桥协议或基于中继链的跨链协议，能够提供更强大的功能和更好的扩展性。

7.2.2 消息格式与传输

7.2.2.1 跨链通信的消息应采用统一的格式，包括消息头和消息体。消息头应包含消息的类型（如跨链交易请求、交易确认、资产查询等）、发送方和接收方的标识（如区块链地址、DID 等）、消息的唯一标识符以及时间戳等信息；消息体应包含具体的跨链操作内容，如交易的资产信息、交易金额、智能合约调用参数等。

7.2.2.2 宜使用基于 TCP/IP 的网络协议，并结合加密技术（如 TLS/SSL 加密）保证消息传输的安全性。同时，设置消息重传和确认机制，防止消息丢失或传输失败。

7.3 智能合约互操作性

7.3.1 合约标准兼容性

应支持不同区块链平台的智能合约标准，实现智能合约在跨链环境下的互操作性。对于以太坊平台的智能合约，应确保其符合 ERC 系列标准（如 ERC-20、ERC-721、ERC-1155 等）。对于其他区块链平台，也应遵循其相应的智能合约标准。

7.3.2 合约调用与执行

7.3.2.1 在跨链互操作中，能够通过跨链通信协议，将智能合约调用请求从一个区块链发送到目标区块链，并在目标区块链上执行相应的智能合约。在调用过程中，应确保调用参数的准确性和安全性，防止恶意调用和参数篡改。

7.3.2.2 应对智能合约的执行结果进行及时、准确地反馈，以便发起调用的区块链能够根据结果进行后续操作。

8 安全要求

8.1 身份认证与授权

8.1.1 用户身份管理

8.1.1.1 应采用去中心化标识符（DID）作为用户在元宇宙资产库跨链互操作中的唯一身份标识。用户通过私钥控制自己的 DID，确保身份的自主性和安全性。

8.1.1.2 应支持多因素身份认证机制，如结合密码、生物特征识别（指纹识别、面部识别等）、硬件令牌等方式，增强用户登录和交易操作的安全性。

8.1.1.3 应将用户的 DID、密码哈希值、生物特征信息哈希值等身份相关数据存储在安全的数据库中，并采用加密技术（如 AES 加密）对数据进行加密存储，只有经过授权的系统组件才能访问和解密这些数据。

8.1.2 权限管理

8.1.2.1 应为不同用户和系统组件分配合理的权限，确保只有经过授权的操作才能执行。采用基于角色的访问控制（RBAC）模型，根据用户的角色（如普通用户、管理员、资产发行人等）定义相应的权限集合。

8.1.2.2 在进行跨链操作时，应严格验证用户的权限，防止未授权的用户进行跨链资产转移、智能合约调用等敏感操作。对于涉及重要资产和关键业务流程的操作，采用多重签名机制，需要多个具有相应权限的用户或系统组件共同签名才能生效，进一步提高操作的安全性。

8.2 数据安全

8.2.1 数据加密

8.2.1.1 在数据传输过程中，应采用 TLS/SSL 等安全协议对数据进行加密。

8.2.1.2 对存储在服务器、数据库等存储设备中的数据进行加密，防止数据泄露。宜采用分层加密策略。

8.2.1.3 密钥生成需通过经检测的密码模块，密钥存储应采用硬件加密保护，同时应建立定期更新机制，以保证密钥的安全性。

8.2.1.4 具备跨链交易端到端的完整性保护，使用安全加密算法对交易信息和资产进行加密保护，同时具备跨链通信端到端的信息加密保护。

8.2.2 访问控制

建立严格的访问控制机制，基于用户身份和权限对元宇宙资产库的访问进行管理。采用角色 - 权限模型，为不同用户分配不同的操作权限（如查询、写入、修改等）。

8.2.3 数据备份与恢复

8.2.3.1 应建立定期的数据备份机制，对资产库中的数字资产数据、交易记录、用户信息等关键数据进行备份。

8.2.3.2 备份数据应存储在安全的异地存储设备或云端存储服务中，以防止因本地存储设备故障、自然灾害等原因导致数据丢失。

8.2.3.3 制定数据恢复策略和流程，在发生数据丢失或损坏时，能够快速、准确地恢复数据。

8.3 智能合约安全

8.3.1 漏洞检测

在跨链智能合约开发和部署过程中，应采用自动化漏洞检测工具和人工审计相结合的方式，对合约代码进行全面的漏洞检测。重点检测合约中的重入攻击、溢出漏洞、权限滥用等安全问题，及时修复发现的漏洞。

8.3.2 安全审计

应定期审查合约的执行逻辑、数据操作和权限管理等方面，评估合约的安全性和合规性。审计结果应形成报告，对发现的问题提出整改建议，并跟踪整改情况。

8.3.3 合约升级与版本控制

8.3.3.1 应建立智能合约升级机制，当需要对智能合约的功能进行改进、修复安全漏洞或适应新的业务需求时，能够安全、有效地进行合约升级。在升级过程中，原有合约的状态应能够正确迁移到新合约中，不影响已有的跨链交易和资产状态。

8.3.3.2 应采用版本控制策略，对不同版本的智能合约进行标识和管理，记录每个版本的功能特性、修改内容和发布时间等信息。

8.4 网络安全

8.4.1 网络攻击防护

8.4.1.1 网络隔离

采用网络隔离技术（如防火墙、虚拟专用网络 VPN），对元宇宙资产库跨链系统的网络进行安全防护，防止外部网络攻击和非法入侵。隔离不同区块链系统之间的网络，限制网络流量的访问范围，降低网络安全风险。

8.4.1.2 流量监控

部署网络流量监控系统，实时监测跨链网络中的数据流量和通信行为，及时发现异常流量和攻击行为（如 DDoS 攻击、恶意扫描等）。通过流量分析和行为模式识别，对潜在的安全威胁进行预警和处理，保障网络的正常运行。

8.4.1.3 安全通信协议

采用安全可靠的网络通信协议（如 SSL/TLS）进行跨链数据传输，确保通信过程的机密性、完整性和身份认证。对通信协议进行定期更新和维护，修复安全漏洞，防止协议被破解和利用。

8.4.1.4 节点安全

应确保区块链节点的安全性，对节点的操作系统、区块链软件进行定期更新和维护，修复已知的安全漏洞。采用访问控制策略，限制对节点的访问权限，只允许授权的设备和用户与节点进行通信。对节点之间的通信进行加密，防止节点间的通信数据被窃取或篡改。此外，应建立节点备份和恢复机制，当节点出现故障时，能够快速恢复节点的正常运行。

9 性能要求

9.1 交易处理能力

元宇宙资产库跨链互操作系统应具备一定的交易处理能力，能够满足实际业务需求。具体的交易处理能力指标应根据应用场景和业务规模进行合理设定。同时，系统应具备良好的扩展性，能够通过增加服务器资源、优化算法等方式，随着业务量的增长灵活提升交易处理能力。

9.2 响应时间

用户发起跨链交易请求后，系统应在较短的时间内给予响应。对于简单的跨链查询操作，响应时间应不超过5秒；对于复杂的跨链资产转移、智能合约调用等操作，响应时间应不超过1分钟。响应时间的设定应充分考虑用户体验和业务流程的要求，确保用户能够快速获得操作结果。

9.3 吞吐量

系统的吞吐量应满足业务高峰时期的需求，能够在单位时间内处理大量的跨链交易和数据交互。在业务高峰时段，系统的吞吐量应不低于50万字节/秒，以保证元宇宙资产库跨链互操作的顺畅进行。通过性能测试和优化，不断提升系统的吞吐量，避免出现系统拥堵和交易延迟等问题。

10 测试方法

10.1 功能测试

10.1.1 资产库功能测试

对资产库的存储、索引查询、验证审核等功能进行测试。验证资产数据能否正确存储到资产库中，通过不同的查询条件（如资产类型、所有者、交易时间等）验证资产索引与查询功能的准确性和效率。模拟不同类型的数字资产进入资产库，检查资产验证与审核功能是否能够有效识别资产的真实性、合法性和合规性。

10.1.2 跨链功能测试

测试跨链协议的管理、消息传递和交易协调功能。验证系统是否能够正确选择和适配不同的跨链协议，确保跨链消息在不同区块链网络之间准确、及时传递。通过模拟跨链资产转移、智能合约调用等场景，测试跨链交易协调功能是否能够保证交易在不同链上的状态一致性，检查是否存在资产丢失、双重支付等问题。

10.1.3 智能合约互操作性测试

测试不同区块链平台智能合约的兼容性和调用执行功能。在跨链环境下，验证以太坊等平台的智能合约能否被其他区块链正确识别和调用，检查智能合约调用参数的准确性和安全性，以及执行结果的反馈是否及时、准确。通过模拟多种跨链智能合约调用场景，全面测试智能合约的互操作性。

10.2 安全测试

10.2.1 身份认证与授权测试

测试用户身份管理和权限管理功能。验证多因素身份认证机制的有效性，模拟用户登录和交易操作，检查身份认证过程是否安全可靠。测试基于角色的访问控制模型，验证不同用户角色是否只能执行相应权限范围内的操作，检查多重签名机制在涉及重要资产和关键业务流程操作时的安全性。

10.2.2 数据安全测试

应检查数据在存储和传输过程中的加密效果，通过模拟数据窃取场景，验证加密数据是否能够有效保护敏感信息。应测试数据备份与恢复流程，模拟数据丢失或损坏情况，检查能否按照制定的策略和流程快速、准确地恢复数据。

10.2.3 智能合约安全测试

对智能合约进行安全审计和漏洞测试。使用自动化审计工具和人工审计相结合的方式，检查智能合约代码中是否存在重入攻击、整数溢出、权限控制不当等安全漏洞。模拟恶意调用和参数篡改场景，测试智能合约在异常情况下的安全性和稳定性。

10.2.4 网络安全测试

测试网络攻击防护和节点安全功能。通过模拟 DDoS 攻击、SQL 注入攻击等网络攻击手段，检查防火墙、IDS、IPS 等网络安全设备是否能够有效防御攻击。测试节点的访问控制、通信加密和备份恢复机制，验证节点在面临安全威胁和故障时的安全性和稳定性。

10.3 性能测试

10.3.1 交易处理能力测试

通过模拟不同规模的跨链交易请求，测试系统每秒能够处理的交易数量。逐渐增加交易请求的并发量，观察系统的性能表现，确定系统的最大交易处理能力。分析交易处理过程中系统资源（如 CPU、内存、磁盘I/O等）的使用情况，找出性能瓶颈并进行优化。

10.3.2 响应时间测试

在不同的业务场景下，测量用户发起跨链交易请求到系统返回响应的时间。分别测试简单查询操作和复杂交易操作的响应时间，分析响应时间与交易负载、网络环境等因素的关系。通过优化系统架构、算法和网络配置等方式，降低响应时间，提高用户体验。

10.3.3 吞吐量测试

模拟业务高峰时期的大量跨链交易和数据交互，测试系统的吞吐量。监控系统在高负载情况下的运行状态，记录单位时间内系统处理的数据量。通过调整系统参数、增加服务器资源等方式，提升系统的吞吐量，确保系统能够满足业务需求。