腾讯安全 Tencent Security | 腾讯领御 安心链接 智慧领御

T-Sec CCGP
跨链协同治理平台

CROSS-CHAIN COLLABORATIVE GOVERNANCE PLATFORM

技术白皮书

V 1.0

腾讯安全领御区块链团队

2021年1月

前言

区块链作为“新基建”的基本建设内容之一，正在各行各业快速、规模化的部署。区块链的密码技术本源和分布式信任属性，梳理归化了信息数据的价值，透明了业务流程规则，在各行各业的内在价值提升、政务治理透明度的增加等方面发挥了核心作用。但是，区块链应用系统的垂直自完备性，导致链上数据的应用以链内循环为主，在链和链间的循环较为困难；链内智能合约支撑的业务规则自动化处理高效，但是，业务流程依赖贯通在链间较难协作。且在产业区块链的实施应用场景中，企业对于链间的互信管理、数据和业务跨链交互等相关的易用性、高效性也有较高的要求。所以，提供一种监管治理下的、高效的企业级链间协同机制，显得尤为迫切。

腾讯安全领御区块链团队从2017年就致力于产业区块链的技术研究、产品开发、解决方案研发。已在区块链中枢平台支撑的智慧城市建设、码链溯源、可信存取证、透明公益等领域推动全自主技术、产品和方案的落地。T-Sec CCGP跨链协同治理平台是腾讯安全领御区块链团队最新打造的产业区块链间协同平台，意在推进区块链间高效互联互通，健全区块链上数据流通治理机制。

T-Sec CCGP跨链协同治理平台面向产业区块链间数据交换、业务协同，并且实施了跨链治理结构，针对政务、企业等应用场景，强调在监管治理下的链间协同。T-Sec跨链协同治理平台在治理链、跨链协同数据管道、分布式中继、流程协议、安全措施等方面进行技术创新，并构建了高安全、易用、高效的企业级跨链全栈解决方案。

“以链治链”，用区块链来管理区块链，回归链的本源来解决链间的协同问题，以“链”作为 “粘合剂”，来拼接数据“拼图”，把一个个后区块链形成的数据“片”，连接起来。我们希望通过企业级的跨链治理平台，与产业区块链上下游用户一起打造广域“数网”的宏伟蓝图。

目录

编委会

（排名不分先后）

指导单位

国家工业信息安全发展研究中心

中国区块链生态联盟

北京邮电大学区块链及安全技术联合实验室

市场咨询

计世资讯

江苏安凰领御科技有限公司

白皮书撰写团队

腾讯安全–领御区块链团队

杨光夫，申子熹，刘鑫，王强，段红杉，
索艳明，冯治波，崔冉，徐文超，刘经程，张伟，仵甘，刘颖

腾讯标准团队

黄超

美术编辑

林如蓝 赵杰

第 1 章. 概述

1.1 CCGP 设计背景

在“数字基建”浪潮的推动下，产业区块链技术、产品与解决方案正在中国各个领域快速的、规模化的部署和应用。其发展具有鲜明的特点，第一、我国产业区块正在减少对国外区块链底层技术的依托，相关的技术架构，区块链存储、加密算法、共识算法等关键性技术的创新催生出多种区块链底层技术平台，呈现出百花其放、“千链争艳”的格局。第二、地域层面产业区块链应用的需求正逐步被放大，在智慧城市、数字治理等业务协同应用中快速部署，区域内物流、供应链、金融信贷等相关实体间信息共享平台逐步建设，地域层面产业区块链应用规模增速正在加快。各级地方政府及行业组织整合各领域、各行业区块链新基建的需求，构建城市级区块链中枢基础设施，并引导本地产业用户的应用迁移到区块链基础设施之上，形成“链上应用”的新趋势。

多样性的产业区块链平台需要统一协作，链与链之间需要“对话”，并进行信息和资产的交换，形成真正的信息价值互通，避免后区块链“信息孤岛”的形成。规模化的区块链应用业务场景要求互通，一些分布式应用系统的业务结果触发另一些分布式系统的业务运行，构建广域的区块链业务应用协作平台，连通更多业务场景，进一步挖掘区块链系统的应用价值。这些需求催生了不同产业区块链平台间以及平台内不同底层架构的区块链应用交互问题，即产业区块链间协同应用，成为区块链基础设施进一步发展建设的刚性需求。

1.2 产品特点

产业区块链进入发展快车道的同时，不同链之间的跨链互操作是亟需解决的技术难题之一。本着科技向善，用户为本的宗旨，我们深入到区块链技术可应用的众多业务场景中进行分析及研究其在跨链互操作方面的业务需求和痛点，提出“以链治链”的跨链互操作模式，即以多方共治的治理链对跨链互操作全流程的治理与管控，构建一个多方共治、高安全、通用易扩展、高效率、留痕可追溯的跨链治理协同平台。

■ **通用易扩展**

在产业区块链跨链业务场景中，参与方多、组网拓扑模型多样、实施限制条件繁多，同时还需支撑同构、异构链的交互需求，显然跨链治理协同平台需具备较强的通用性及易扩展性。

我们围绕通用易扩展这一产品设计理念，提出了面向产业区块链通用的跨链治理协同平台，分布式的中继服务可适配同构、异构链的接入，提供通用标准化的接入通道，可横向动态接入参与方、纵向动态互通治理，可平滑支撑多种组网拓扑模型，极具高通用性和易扩展性。同时实现了带有权限、多阶段、分布式的管道协议，使跨链协同交互具备极高的易用性。

■ **多方共治**

我们发现在产业区块链业务需求场景下，对跨链协同的需求具有参与方之间需具备强信任基础、跨链交易过程透明、跨链权限可管控、跨链可追溯等特点，基于这些需求维度，跨链参与方之间可形成更好的业务协作互信体系。我们提出了以区块链为手段建立多方共建、共治的协同平台。

■ **高效**

跨链互操作的使命是构建区块链之间的通信网络，消灭数据孤岛，在区块链网络间传递信任，构建区块链价值互联网。在产业区块链业务场景下，大数据量的跨链互通是其重要特点之一，具备高效率的交易处理能力已然成为跨链互操作平台的标配。

CCGP在架构上实现了治理模式下的大规模组网、分布式中继服务，使得交易通信及验证更加高效，在“以链治链”的设计理念下，依托于治理体系的权限管控能力，使得整个跨链处理过程中权限的验证流程简化、通信高效。

■ **高安全性**

跨链协同治理平台需保障参与方身份、业务数据、跨链通信过程、合约安全合规等方面的高安全性。CCGP从通信安全、安全沙箱中间件、证书合规、合约审计、密钥管理、节点与跨链中继服务的可信防护环境以及跨链权限管理等方面进行安全性架构设计，以保障跨链互操作全流程的高安全性。

■ **留痕可追溯**

产业区块链跨链服务平台的构建是建立在信任基础之上的，从我们调研的需求场景中发现，除了通过交易验证等技术手段实现跨链交易的确认之外，对跨链交易的留痕、审计及追溯也是常见的刚性需求。

基于此，我们提出了在治理链上通过智能合约实现对跨链交易台账的记录以及交易事务终态的确认，同时提供跨链交易的留痕、追溯、异常预警以及最终一致性对账机制等功能。

第 2 章. CCGP 整体架构设计

2.1 整体架构及核心流程

在对产业区块链跨链协同业务需求场景的深入研究之后，我们对各行业跨链业务需求进行综合分析并进行标准化设计，提出“以链治链”的通用跨链协同治理架构，其治理结构图、总体架构图如图1、2所示。

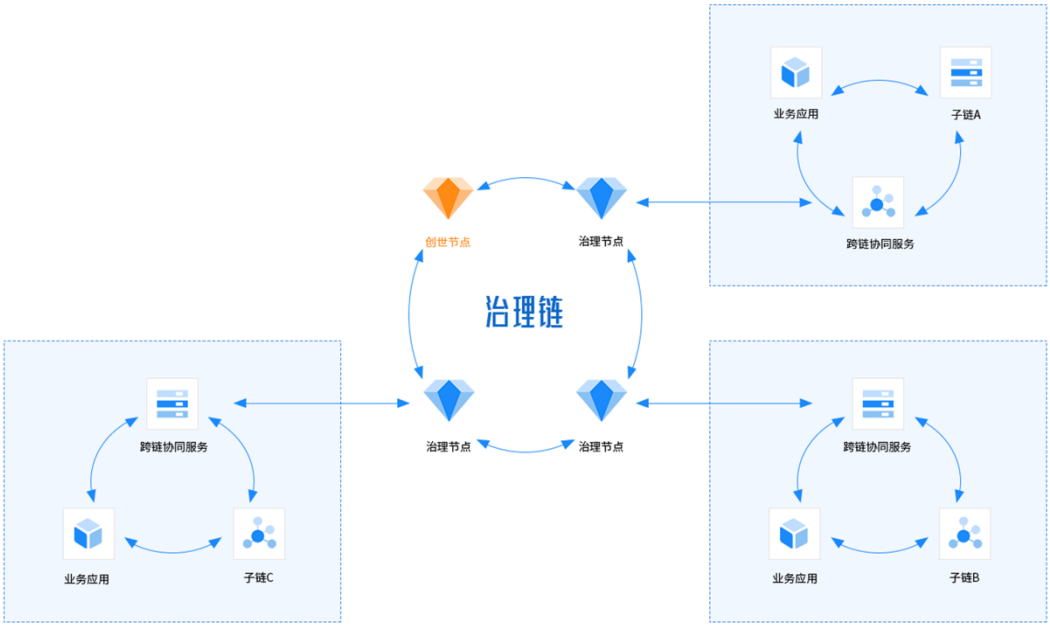

图1 治理结构图

CCGP治理结构中包括治理链、子链、业务应用及跨链协同服务等对象，各子链间、业务应用与链之间通过跨链协同服务执行跨链互操作，治理链实现跨链协同全流程的管控。

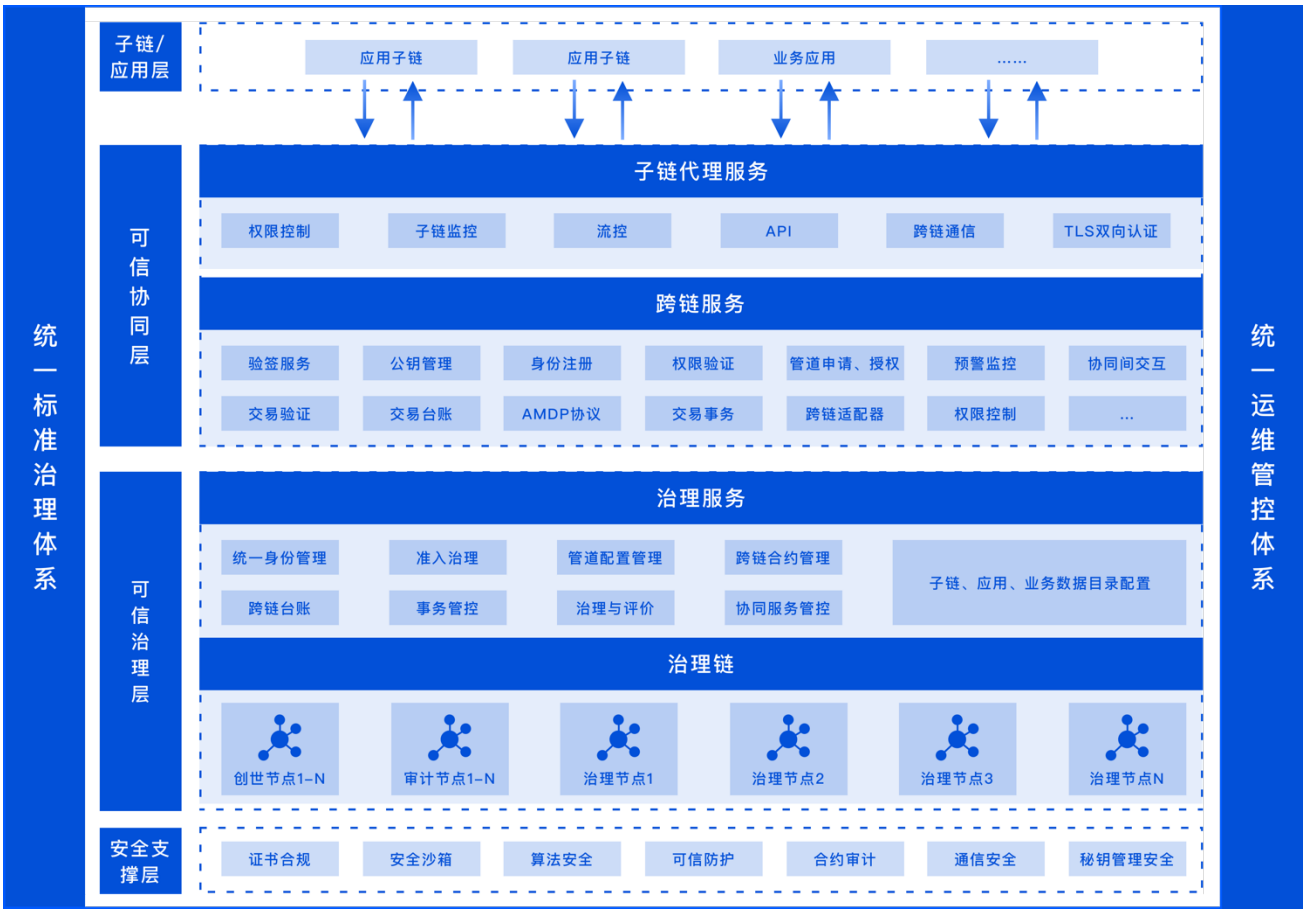

图 2 总体架构图

CCGP总体架构共包含四层两体系，分别为安全支撑层、可信治理层、可信协同层、子链应用层、统一标准治理体系以及统一运维管控体系。

安全支撑层为整个跨链协同治理提供安全保障；可信治理层提供跨链协同全流程的治理管控服务；可信协同层提供跨链互操作的服务能力；子链应用层为跨链互操作的各参与方；统一标准治理体系为CCGP提供协同治理标准规范；统一运维管控体系为CCGP提供平台运维及管控的标准规范。

跨链互操作流程分为业务应用与链之间、链与链之间两种模式，两种模式下的跨链协同治理交互过程基本相同，主要区别在于跨链发起者不同，业务应用与链之间的跨链互操作中，发起者是业务应用；链之间的跨链互操作中，是通过监听目标链上有跨链相关的新交易产生时而触发的，核心交互流程如图3所示。

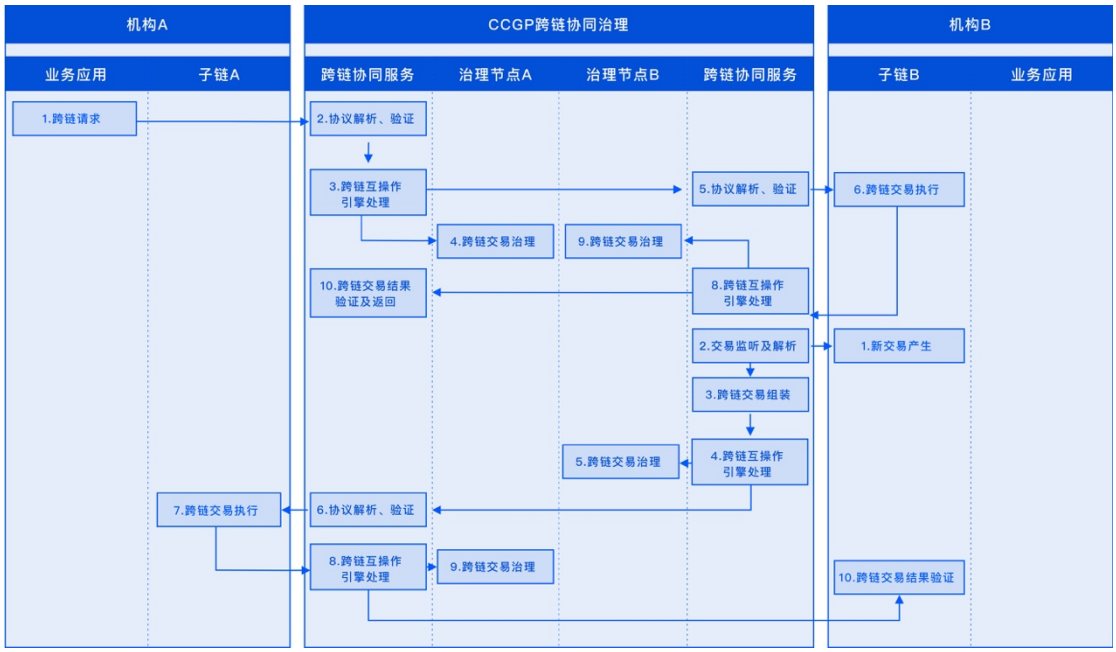

图3 跨链互操作流程

2.2 可信治理

■ 2.2.1 治理链

治理链是基于区块链技术特性实现跨链协同全流程管控的一条区块链。

治理链成员机构主要由创世机构、业务方机构和监管审计机构组成。治理链节点分为创世节点、治理节点和审计节点；创世节点是由创世机构持有；治理节点是由参与到跨链业务机构持有；审计节点是由监管审计机构来持有，如图4所示。

治理链运行后，创世机构中的治理员初始化治理合约，这些合约主要包括对机构、账户和跨链业务管控即业务数据直接存储在链上，基于链上进行同步分布式存储。管理治理节点的机构进行跨链业务操作。

治理链记录所有参与跨链业务机构的台账交易数据，便于后期追溯。

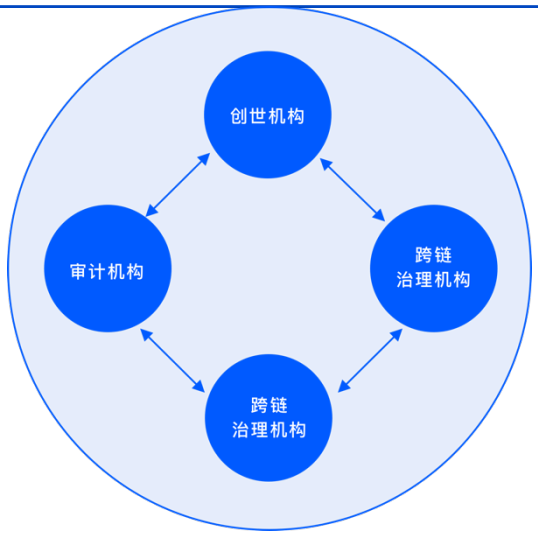

图4 治理链

- **2.2.1.1 创世机构**

创世机构是指跨链联盟中承担跨链治理角色的机构。

- **2.2.1.2 跨链治理机构**

具有跨链协同需求的业务方机构向治理链提出加入申请，由跨链创世机构投票表决通过后，该业务方机构即成为跨链治理机构。

- **2.2.1.3 审计机构**

对平台中所有跨链协同业务过程进行审计的机构称为审计机构。

- **2.2.1.4 创世节点**

治理链中，创世机构持有的区块链节点为创世节点。通过创世节点执行创世合约部署管控、授权跨链业务方调用、协同治理等合约交易。

- **2.2.1.5 治理节点**

治理链中，跨链治理机构持有的区块链节点为治理节点。跨链业务机构通过治理节点参与协同治理共识，为跨链业务提供管控通道。

- **2.2.1.6 审计节点**

治理链中，审计机构持有的区块链节点为审计节点，该节点不参与共识，只具备同步治理链上数据的权限。

- **2.2.1.7 业务机构接入**

接入机构需向CCGP提出接入申请，申请时需提交身份、机构类别、业务属性等信息，现有创世机构成员对接入的机构进行投票决策，决定是否同意其加入。CCGP平台会给被批准接入方机构颁发统一身份标识。

- **2.2.1.8 统一身份管理**

CCGP 中参与操作的角色分为：治理员、业务方账户、审计员，在治理链体系中，采用统一账户身份管理，通过治理链上身份治理合约进行权限管控。

- **2.2.1.9 投票治理管控**

系统新增账户时，所有当前创世机构成员投票通过，新增账户才能生效。流程如下：

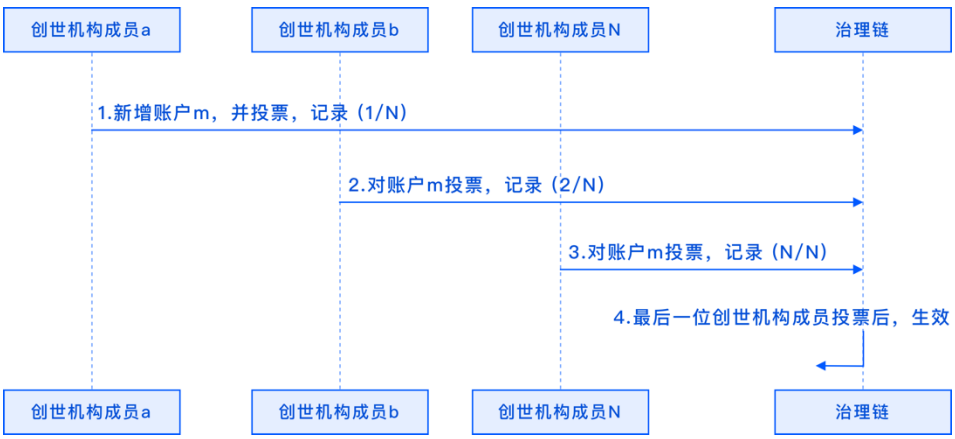

图5 新增账户流程图

■ 2.2.2 治理服务

治理服务主要支撑治理员、审计员对治理链及治理协同业务进行管控操作。治理服务分为服务层和控制层，在服务层提供了权限控制和接口API，在控制层主要提供治理合约管理、跨链机构管理、统一身份管理、节点管理、协同服务管控、子链管理、应用管理、管道管理、台账管理、数据同步、治理同步监控和治理业务管控等，如图6所示。

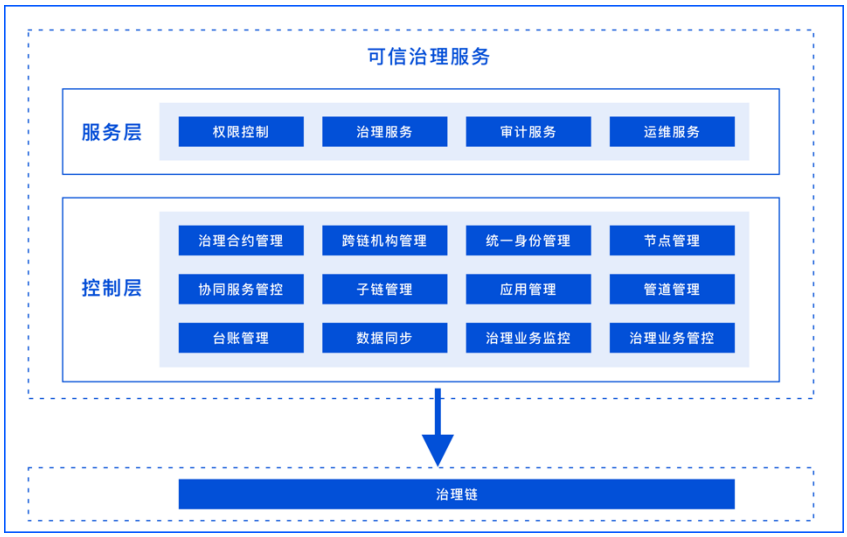

图6 可信治理服务架构图

● 2.2.2.1 服务层

在可信治理服务层中，需要对不同角色权限进行控制，并提供治理服务、审计服务和运维服务。

● 2.2.2.2 控制层

- **治理合约管理**

治理链部署完毕后，初始化支撑协同治理全过程的智能合约，核心合约如下。

序号	名称	描述
1	机构管理合约	管理治理链上所有机构信息
2	协同服务管理合约	管理治理链上所有协同服务信息
3	账户管理合约	管理治理链上所有账户信息
4	投票工单合约	治理链上投票工单合约
5	管道合约	治理链上跨链管道管控合约

- **跨链机构管理**

主要指治理机构的新增及维护。

- **统一身份管理**

CCGP根据用户角色和权限不同分为治理员、操作员和跨链账户。治理员是由CCGP联盟协商确定。如图7所示。

图7 权限设计

- **节点管理服务**

在CCGP中，治理员可对跨链治理节点的状态进行管控。

- **协同服务注册**

在CCGP中，治理员将协同服务部署环境的IP、端口和唯一标识等信息进行注册绑定。

- **数据服务**

在CCGP中，对子链属性信息、跨链应用、管道属性和台账进行查询。

- **治理业务审计**

对参与跨链的所有业务进行异常行为和风险的审计服务。

- **治理业务管控**

发现异常跨链治理业务并对其进行限制处理。

- **数据同步**

通过数据仓库工具对治理链上数据进行同步分析处理。

2.3 可信协同服务

可信协同服务是承接跨链业务处理的主要服务中枢，其功能不仅连接子链与治理链，同时也承载着可信协同服务点对点的跨链互联。

可信协同服务分为子链代理服务和跨链代理服务，两个服务之间相互独立，保证跨链业务逻辑的安全可信，同时也保证子链通信的安全、灵活，易扩展。

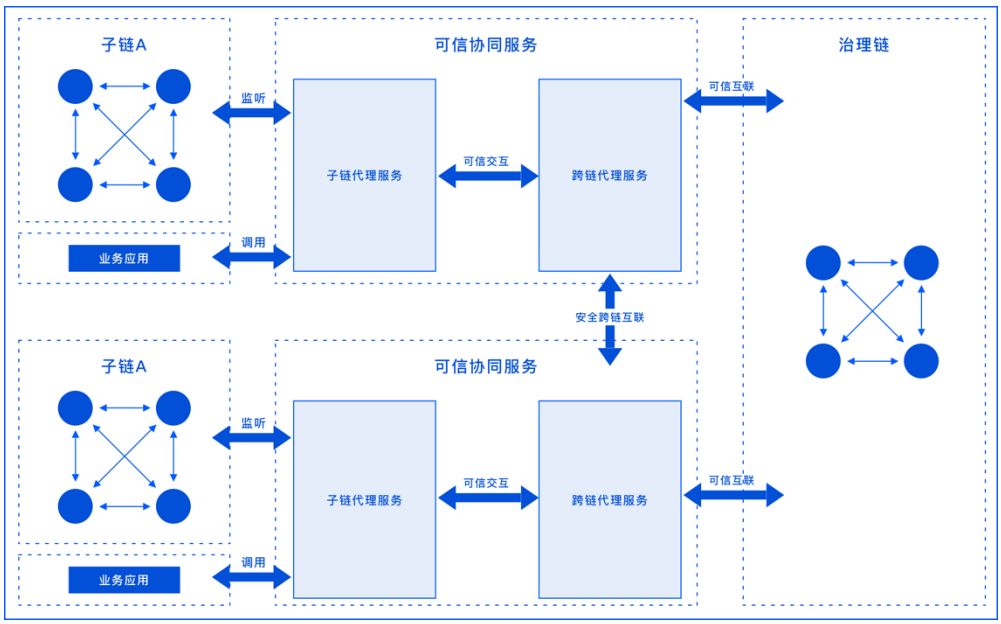

图8 可信协同服务结构图

■ 2.3.1 子链代理服务

子链代理服务负责与子链通讯、与跨链代理服务可信数据交互。子链代理服务以插件形式，支持与不同子链进行安全的交互，其主要功能包含控制层和服务层。服务层提供权限控制层、流控、接口API以及跨链代理服务通信等。控制层提供子链监控、子链数据监听同步、子链跨链交互、当前服务监控、跨链代理服务监控、跨链数据管理以及跨链代理服务通讯等。

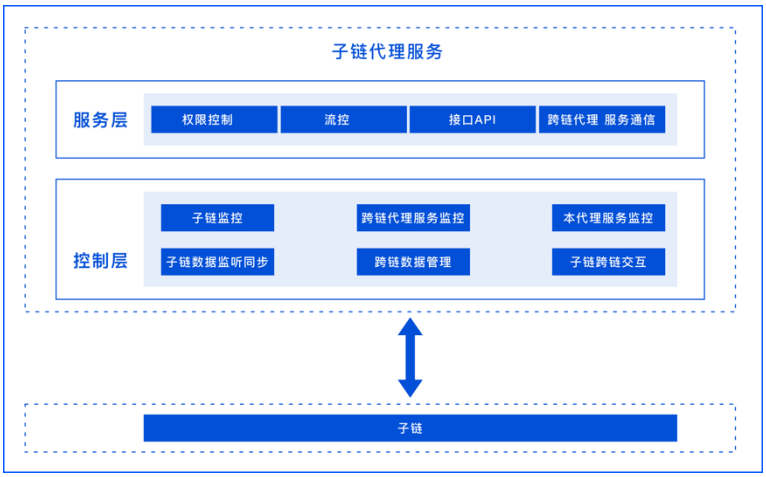

图9 子链代理服务架构图

系统抽离出通用的子链集成通信接口，针对不同的子链只需要实现对应的接口就能够完成子链与子链代理服务的通信，子链代理服务通过插件方式动态加载不同子链。

- **2.3.1.1 服务层**

子链代理服务中，需对业务应用请求做权限及流量控制，并对外提供相应的API接口。同时，需提供与跨链代理服务交互接口API及权限控制。

- **2.3.1.2 控制层**

- **子链监控**

通过子链接口，实时获取子链运行状态及业务状态。

- **跨链代理服务监控**

因子链代理服务与跨链代理服务间有网络通信，为保证业务的可用性，子链代理服务需监控跨链代理服务的运行状态。

- **本代理服务监控**

为保证子链代理服务的可用，子链代理服务实时提供当前服务的运行状态及设备状态。

- **子链数据监听同步**

通过订阅及区块高度的同步的方式，实时同步链上数据，并根据业务需求解析所需数据。

- **跨链数据管理**

管理子链跨链的业务数据。包含有来自业务应用及监听同步的数据。

- **子链跨链交互**

包含子链主动发起的跨链交互及被动来自于跨链代理服务的跨链交互。

■ 2.3.2 跨链代理服务

跨链代理服务是跨链业务的核心处理服务，也是连接子链代理服务、跨链代理服务、治理链的桥梁。跨链代理服务包含控制层和服务层。

跨链代理服务会监听、同步治理链上的数据，根据治理链上的权限配置做相应的业务处理。一个跨链代理服务唯一匹配一个子链代理服务，AMDP是跨链代理服务与子链代理服务之间的交互协议，保证子链代理服务和跨链代理服务之间数据交互的安全可信。

跨链代理服务可以根据管道寻址（详见2.4），找到目标跨链代理服务的访问信息，建立跨链代理服务间的通信。

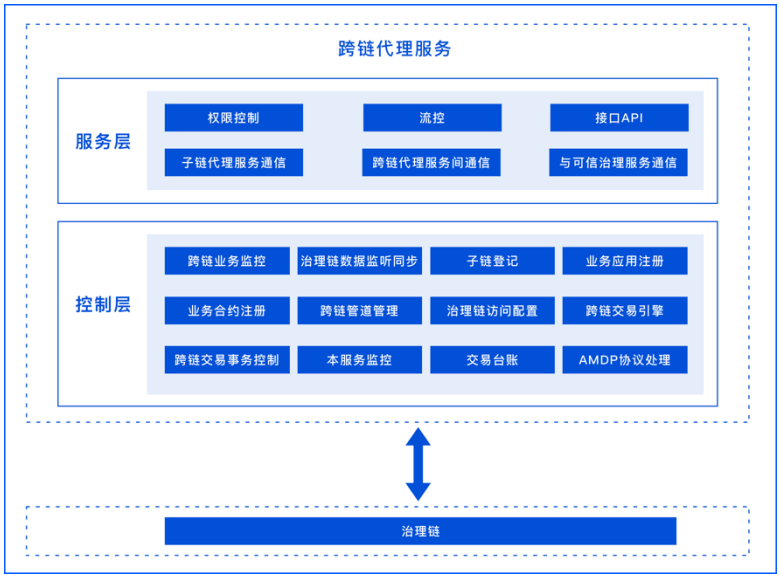

图10 治理代理服务架构图

- **2.3.2.1 服务层**

跨链代理服务中，需对子链代理服务的请求做权限及流量控制，并对外提供相应的API接口。还需提供跨链代理服务间交互接口API及权限控制。

- **2.3.2.2 控制层**

- **跨链业务监控**

  实时获取治理链运行状态及业务状态。

- **治理链数据同步**

  实时同步链上数据，并根据跨链规则解析数据。

- **子链登记**

  接入方自主登记子链信息。

- **业务应用注册**

  接入方自主注册本方业务应用。

- **业务合约注册**

  接入方自主注册本方业务合约信息。

- **跨链管道管理**

  申请及授权管道权限。

- **治理链访问配置**

  初始化跨链代理服务访问治理链的相关配置。

- **跨链交易引擎**

  跨链交易数据包的传输及处理。

- **跨链交易事务控制**

  控制跨链交易事务的完整性、一致性及补偿机制。（详见2.5）

- **本服务监控**

  提供自身服务的实时运行状态及设备状态。

- **交易台账**

  提供跨链业务交易台账查询服务。

- **AMDP 协议处理**

  解析并处理跨链协议。（详见2.4.1）

2.4 跨链可信管道

CCGP中，链与链之间的跨链业务交互需要通过管道来传递，管道的属性则决定两个子链之间某一特定业务在跨链互操作时所需的必要条件。

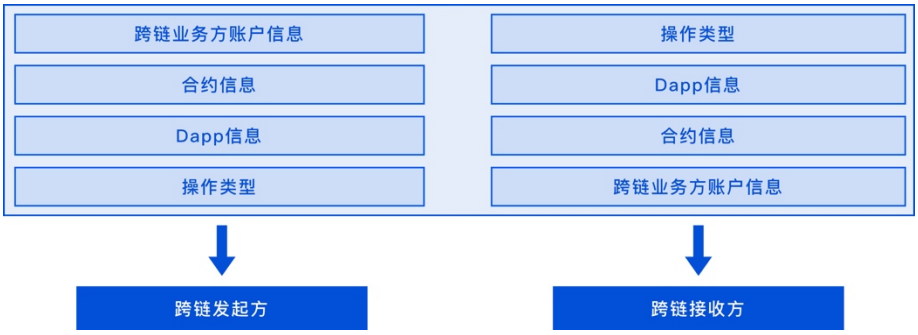

图11 管道属性信息

如上图所示，一条完整的管道由跨链双方相关的属性信息组成，属性信息包括跨链双方的身份信息及治理链上跨链交易合约信息。

■ 2.4.1 跨链协议 AMDP（Authorized Multi-Stage Distributed Protocol）

CCGP设计了一套面向产业区块链间的跨链协议，协议涵盖权限验证、数据完整性校验、跨链互操作交互流程等。

跨链互操作过程中，AMDP需要跨链管道的约束信息为基础进行交互，管道约束信息包括权限信息（跨链双方账户信息）、业务路由信息（跨链服务位置信息，业务合约信息）。AMDP跨链协议需要声明管道约束信息，跨链交易数据、交易凭证及数字签名。管道约束信息和交易凭证用于跨链交互中的权限判断，安全验证。

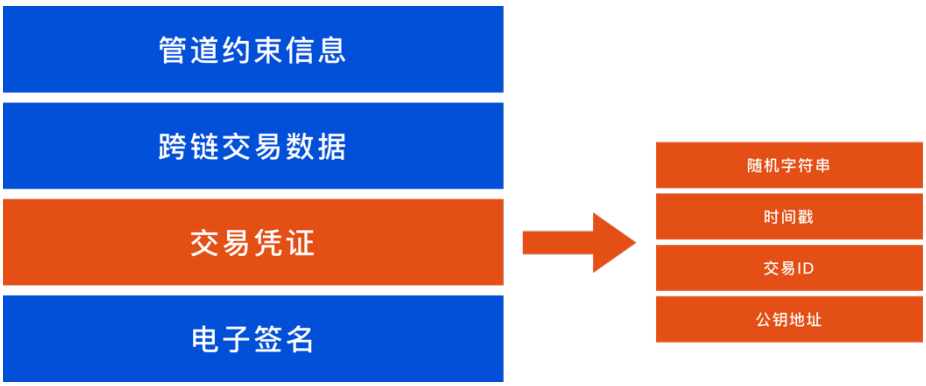

图12 跨链通信协议内容

■ 2.4.2 带业务权限、多阶段、分布式协议

AMDP跨链管道协议分为多个阶段在分布式对象上执行，整体流程如图13所示。

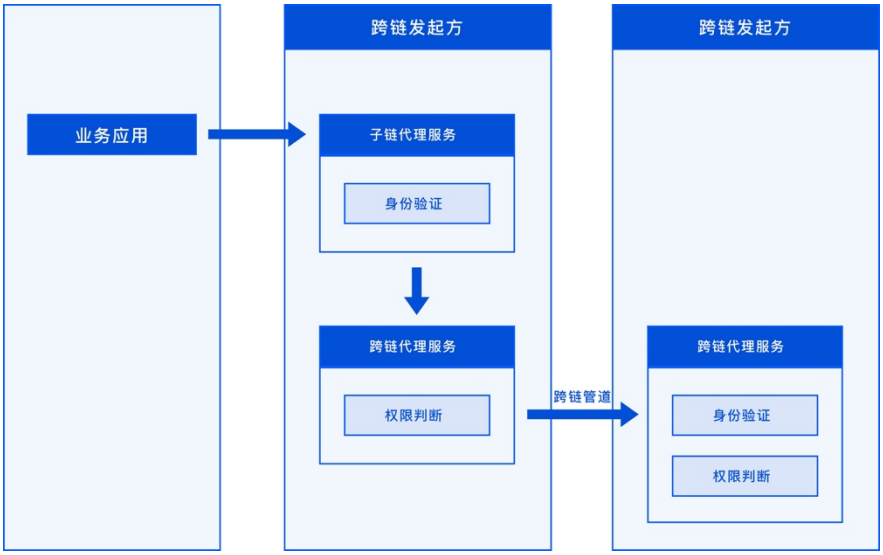

图13 跨链协议整体流程图

1. 跨链业务应用与子链代理服务交互

跨链发起方在进行跨链交易时，先由跨链发起方的业务应用调用子链代理服务，发起第一阶段的跨链通信。本阶段中，业务应用将预先配置的非对称密钥对对应的公钥地址放入交易凭证中，并通过对应的私钥对协议数据包做数字签名。

子链代理服务在接收到业务应用的请求后，解析协议中的管道约束信息，并根据交易凭证中业务应用提供的公钥地址，匹配管道搭建时业务应用预留的公钥，该公钥会用于本阶段跨链协议的业务应用身份验证，以及跨链数据的完整性校验。

2. 跨链代理服务之间的交互

跨链发起方在完成第一阶段的跨链通信后，请求将转发到跨链发起方的跨链代理服务。跨链代理服务会解析协议中的管道约束信息，对本次跨链发起方的业务应用做权限判断。在权限判断通过后，跨链发起方会根据管道约束信息中的业务路由寻址匹配跨链接收方的代理服务并发起第二阶段的跨链通信。在本阶段中，跨链发起方将内置的公钥地址放入交易凭证中，并通过业务账户对应的私钥对跨链数据包做数字签名。

跨链接收方的治理代理服务在收到发起方的跨链请求时，会解析协议中的管道约束信息，并根据交易凭证中跨链发起方提供的公钥地址，匹配管道搭建时跨链发起方预留的公钥，该公钥会用于本次本阶段跨链协议的跨链发起方身份验证，权限验证，以及跨链数据的完整性校验。

2.5 跨链互操作事务控制

跨链交易流程的完整性，一致性需要事务管理来控制。在跨链交易流程中，出现其中一方失败或者异常时，应该由跨链事务的异常处理介入该次跨链。为避免过多的改造子链业务合约，我们将复杂的事务处理逻辑放到治理链中，通过治理链的事务治理合约来完成对跨链操作事务的控制。

为保证跨链交易的事务的正常控制，我们将跨链交互中对子链的操作分为了两个原子性操作：写操作和读操作。原子操作结束后，调用事务合约，将原子操作结果记录到治理链事务控制中。AMDP协议完整流程包含对多个子链的读写操作。

■ 2.5.1 事务控制流程

在跨链流程中，所有的原子操作都需要向治理链发送执行结果，治理链在事务中记录跨链操作状态，跨链互操作事务控制流程如图14所示。

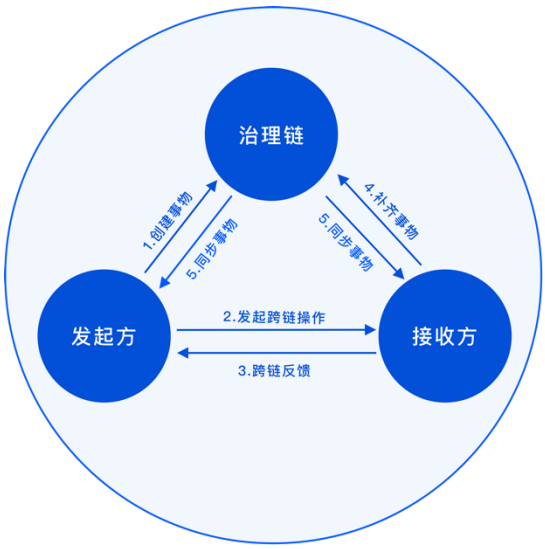

图14 事务控制流程

跨链操作开始后，跨链发起方开启事务控制，并调用事务治理合约创建事务记录。事务开启后，跨链发起方通过AMDP，向跨链接收方发起跨链操作。

跨链接收方在接收到跨链请求后，需要先根据交易凭证查询本交易发起方提交的事务状态，如查询到事务存在失败或异常情况，则停止本次跨链操作，并补齐事务；如前半段事务无异常，跨链接收方会在处理完相关跨链操作后，将跨链操作结果反馈给跨链发起方，并将在本方的原子操作结果补充到事务记录中。

在事务补齐后，跨链代理服务会同步最新的事务记录，并进行跨链互操作验证。

■ 2.5.2 跨链互操作验证

跨链互操作的相关凭证都会记录到治理链中。校验方从治理链中获取相对应的跨链互操作凭证，然后到相应的子链上进行查询校验，若验证结果异常则执行事务补偿操作。

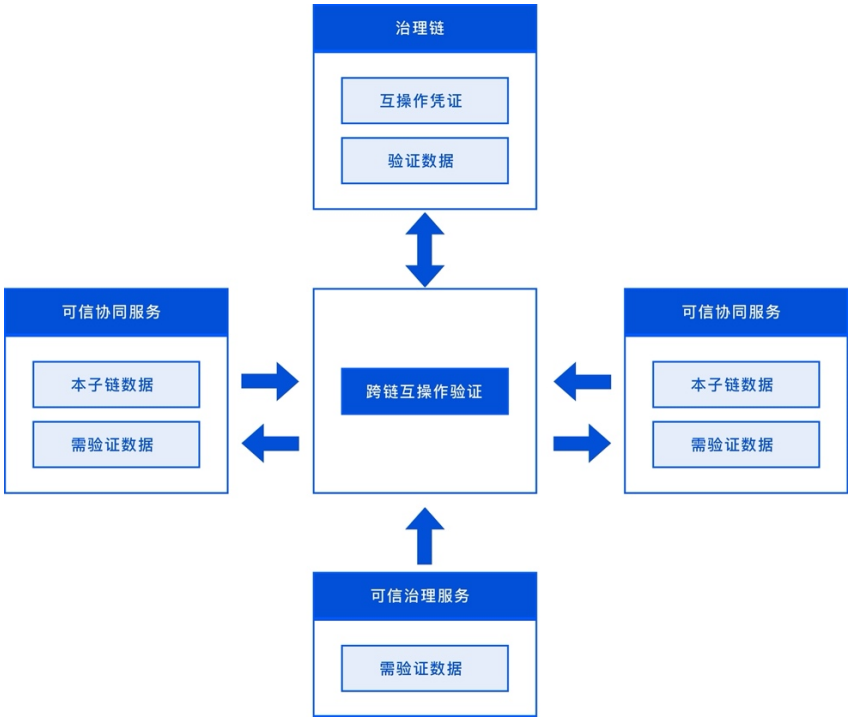

图 15 互操作验证流程

■ 2.5.3 事务补偿机制

跨链互操作验证不存在异常，则视为本次跨链操作完成；若存在异常时，治理代理服务需要启动事务补偿机制，如图16所示。

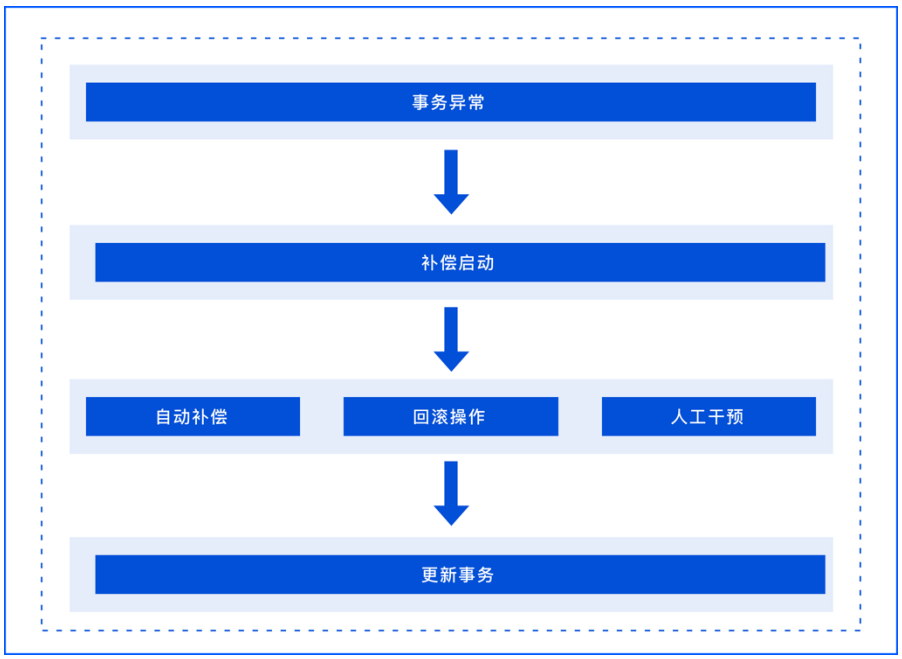

图16 事物补偿机制

根据跨链交易执行发生的异常或失败的具体情况进行自动补偿（如心跳抖动等）、回滚操作（子链业务数据不具备完成跨链交易）或人工干预（宕机，网络断开等）相结合等多种补偿处理方式。

补偿操作过程中，治理代理服务调用事务治理合约，将最新的事务处理结果同步到事务记录中。

第 3 章. 跨链治理及评价

3.1 跨链治理模式

“以链治链”是CCGP跨链治理模式的全面概括，我们提出了以治理链为多方参与共治的跨链基础通道，实现了对机构方、审计方、业务方投票决策式的准入机制；对治理员、审计员、业务方账户、业务应用等身份的动态管理；对治理合约的调用权限的授权管理；以及对跨链交易过程的监控管理。

3.2 治理可视化

治理可视化是将跨链治理相关的业务数据以可视化的方式展现出来，便于直观的查看治理业务数据的相关情况。也为运维、监控提供了相应的指标。治理可视化包含：治理链监控、治理业务管控、跨链交易管控及跨链业务监控。

治理链监控：链的基础数据，如最新区块高度、最新出块时间；治理节点数等

治理业务管控：治理合约数据、跨链机构数据、跨链节点数据等；

跨链交易管控：接入的子链数、管道总数、跨链合约总数等；

跨链业务监控：跨链交易台账、跨链待办数据等；

3.3 跨链治理信用度评价

CCGP引入了跨链治理信用度评价体系，实现了对各参与方跨链行为的治理评价，根据评价结果得出各参与方的综合信用值，对低于信用阈值的对象进行权限管制或清退等操作，可有效防控参与方的“作恶”行为。

第 4 章．跨链治理安全保障

跨链治理能力安全保障，是一套集算法、安全沙箱、通信链路、证书管理服务、跨链治理服务及节点可信计算环境等的整体防护配置策略。

4.1 算法安全

区块链中核心密码算法主要为杂凑密码算法及非对称密码算法。其中杂凑密码算法主要用于地址派生、创建唯一标识符、保护块数据、保护区块头、生成Nonce。非对称密码算法主要用于对交易进行数字签名、公钥派生地址、验证交易签名、加密用于验证交易发起方身份真实性。

随着量子计算机技术的兴起，众多的公共密钥密码系统面临着被量子计算破解的风险。量子计算机可加快非对称算法的破解攻击速度，可以有效地将密钥长度减半。 摘自 NIST IR 8105 出版物，以下常用的密钥算法将不再安全，涵盖对称算法、Hash算法及非对称算法。NIST列举了例如AES、SHA-2、RSA、ECDSA,ECDH、DSA等算法已不具备抗量子攻击的能力。

因此，我们的跨链治理服务在算法安全性设计中，除支持国产商用密码算法外，还采用了可以抵御量子计算环境攻击的密码算法。相关算法如下：

ECDH and ECDSA NIST P-384曲线

SHA-384/512

AES-256

RSA 3072-位或者更长

Diffie-Hellman 3072-位或者更长

4.2 安全沙箱

为了能更安全的管理、应用、存储核心密钥，跨链治理服务应用了高安全硬件级别的密钥存储沙箱及可信密钥计算环境，保证密钥计算在安全环境中运行。我们设计一个软件TPM使用SGX来实现整个密钥存储及计算环境的安全性保障。名字定义为TPM-SGX，对外提供套接字 API 来为应用程序提供服务功能。

通过在硬件上引入可信芯片，从结构上解决区块链跨链治理服务系统和节点在安全方面的脆弱性问

题。在制造安全芯片时，在TPM（可信平台模块）的安全芯片中永久内置签名密钥对的私钥，该私钥永远不能导出TPM，有效保护节点身份安全。

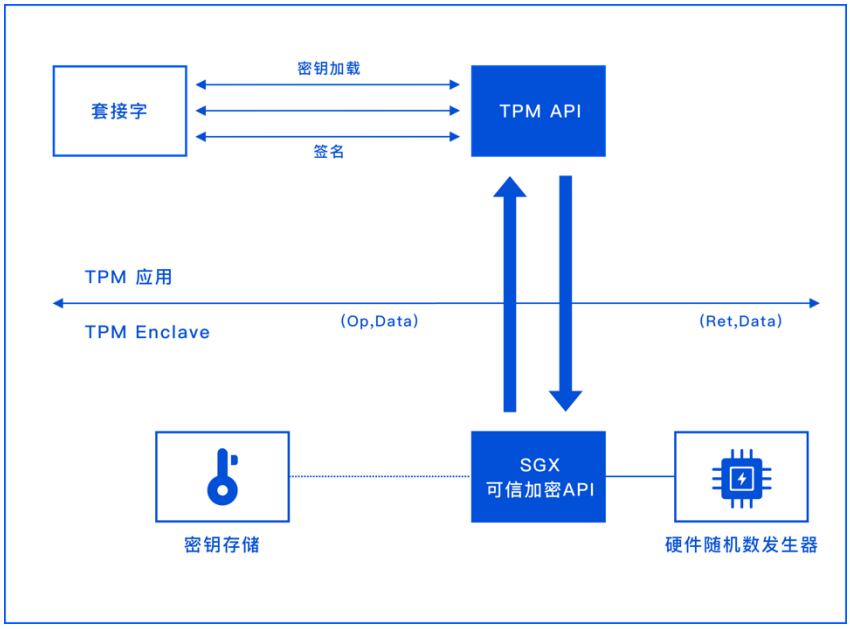

图17 安全沙箱处理流程

4.3 密钥管理安全

跨链治理服务通过高安全级别的密钥管理服务（Key Management Service）来保证密钥的生成、分散、应用。通过安全链路，将根密钥及业务密钥下发至RoT（TPM）芯片中。

通过密钥管理服务，将核心密钥从生成、分发、旋转、存储、终止和存档各个阶段的全流程生命管理，实行安全地管理、处理和保存加密密钥。设计架构如下图18所示：

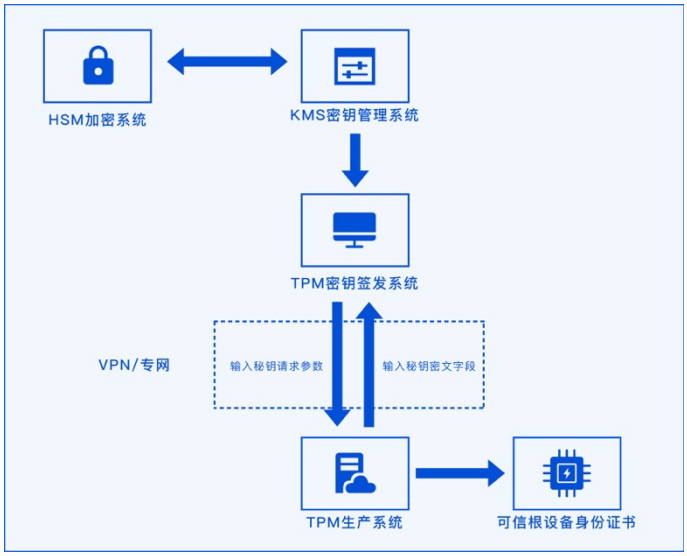

图18 跨链治理密钥管理服务

4.4 证书合规

跨链治理服务通过引入PKI认证体系，实现核心节点的身份鉴权，与数据完整性校验，保证核心节点服务建立在可靠的安全及信任基础之上。通过PKI/CA体系，保证治理链节点及前置机的身份认证和授权。

机密性：基于PKI技术的数字证书，可保护传输数据和静止数据的机密性。确保每个节点的数据加密传输到正确的节点上，只有拥有私钥的节点才可以访问获取数据。

完整性：PKI技术可以确保所有从终端节点中传入或传出的数据无法被篡改，保护从终端节点或其他智能系统获取的数据的完整性。

身份认证和授权：CA证书提供比其他方案更强大的客户端身份验证，为每个终端节点及用户提供唯一身份认证，以便进行细粒度管理，并基于证书实现授权管理。

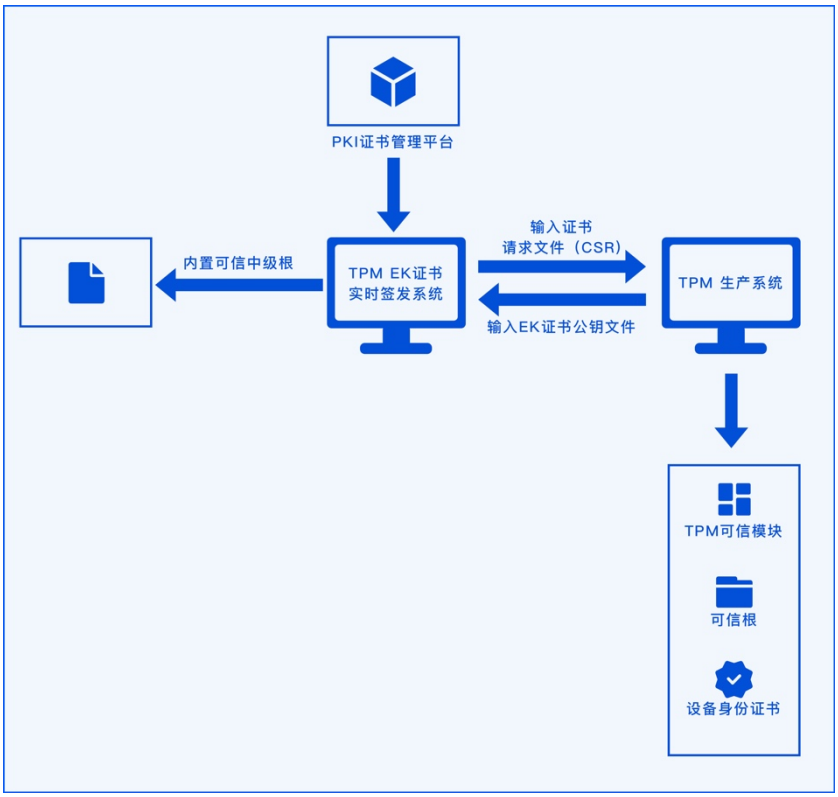

图19 跨链治理可信证书管理服务

4.5 节点、前置机可信防护环境

可信计算是一种安全防御技术. 它利用硬件属性作为信任根，系统启动时逐层度量，建立一种隔离执行的运行环境，保障计算平台敏感操作的安全性，从而实现对可信代码的保护。通过在计算节点中集成专用硬件模块建立信任锚点，利用密码学机制建立信任链，构建可信赖的计算环境，从根本上解决计算平台的安全问题。

通过在接入区块链节点上内置TPM安全信任根，对节点的激活，准入及业务流程提供一体化可信安全操作，同时基于区块链跨链治理服务，对区块链节点、前置机系统安全及应用程序完整性提供白名单管控、进程管控、实时报警监控等可信环境防护功能。

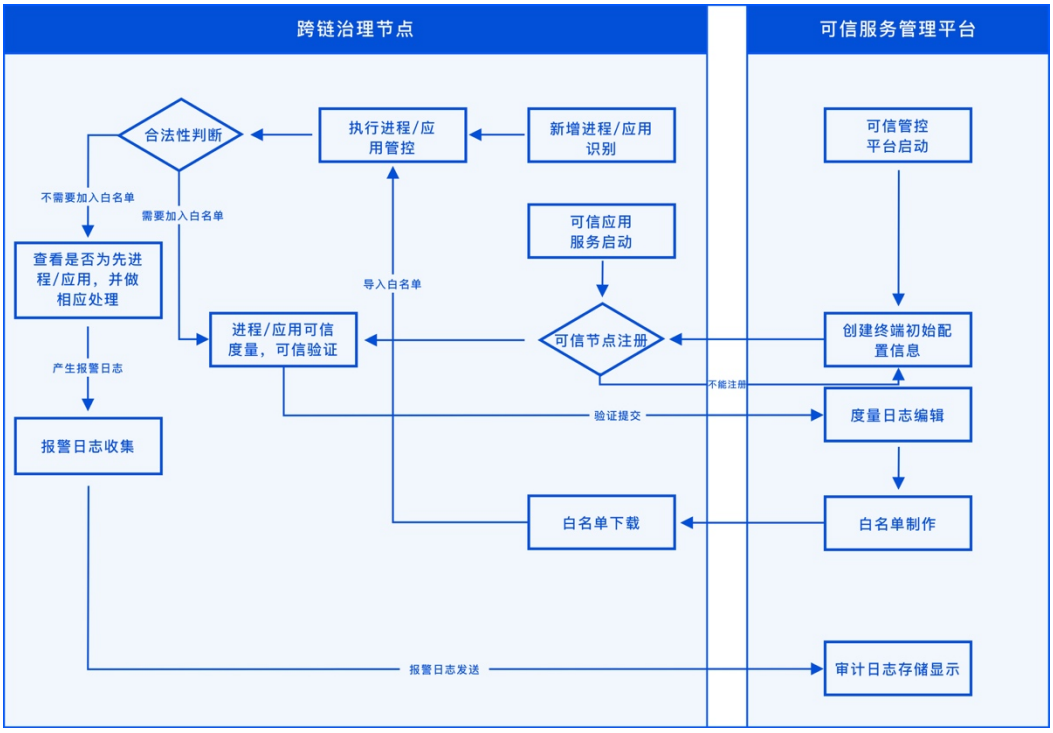

图20 可信防护环境处理流程

跨链治理服务采用的节点安全防护产品基于可信环境技术，业务系统主要分为区块链区块链节点（终端防护）和可信服务管控平台两大部分，两者相互之间的主要业务包括注册认证、可信度量、可信信息验证、白名单发布、审计日志传输等流程，设计思路如上图所示：

1、跨链治理区块链可信节点终端自动跟踪记录主机启动过的进程、正在使用的活动进程，并且能够通过可信验证功能主动识别安装在可信区块链节点上的软件及应用进程。通过TPM 可信计算芯片，将上述进程逐一进行可信度量并将度量信息加密后存储到TPM芯片中；

2、白名单相关数据信息将采用可信存储技术进行保护，进而阻止攻击者篡改或重放白名单；

3、可信区块链节点根据度量的进程信息向可信服务管控平台提交生成进程白名单的请求，这份白名单请求必须经过安全管理员的审核批准后才会最终在跨链治理区块链节点终端生效；

4、跨链治理区块链节点将白名单应用到进程管控功能中，基于可信环境验证计算技术实施程序进程的白名单管控，阻止白名单外的其他进程的运行；

5、跨链治理区块链可信节点实时监控、检测主机运行应用情况，如遇到非法进程试图启动则会将其阻止并向可信管理服务器发送报警日志。

4.6 通信安全

CCGP应用服务与跨链代理服务、跨链代理服务与子链代理服务、跨链代理服务与治理链、治理链节点之间通信均使用TLS协议，以确保各实体间通信的机密性。TLS协议为实体提供三种服务，即：加密、身份验证和完整性保护，在CCGP中使用三种应用模式：

加密——隐藏从一个实体传输到另一个实体的信息;

身份验证——验证传输信息的实体的身份;

信任——检测信息是否被伪造。

TLS握手过程协议，建立实体和实体的身份的真实性连接。加密安全数据通道在实体间建立，连接实体须就通信中所使用的加密方法和密钥匹配。通信过程中使用公钥加密，实体在没有彼此任何先验知识的情况下建立共享秘密加密密钥。实体的密钥私钥在硬件HSM或者TPM中保护，提供防本地物理攻击的、面向金融应用安全级别的高等级防护。

4.7 合约审计

智能合约作为区块链应用中最主要的技术特征，其在设计时容易存在漏洞，且一旦上链将无法更改。而这些漏洞很容易成为黑客攻击的对象，造成大量经济损失，甚至严重影响区块链的稳定运行。因此，确保区块链数据可被信任及安全有效地传输，提供区块链安全监管服务以及智能合约全生命周期的防护，已成为产业区块链系统安全的必要防护手段。

CCGP平台提供安全沙箱，用于测试智能合约的功能，支持智能合约的编写、编译、安全性评估等过程的执行。CCGP提供智能合约细粒度自动化漏洞检测技术，实现适配多类型智能合约的深度安全防护方法和技术。

第一、自动识别智能合约代码“关键”路径，对程序路径进行优先排序，并对智能合约的关键路径进行模拟运行全覆盖，自动过滤不可行的执行路径。

第二、根据知识库对合约潜在的污点进行识别，识别污点信息在智能合约中的产生点并对其进行标记，按照实际需求和污点传播规则进行前向或后向数据依赖分析，得到污点的数据依赖和被依赖关系的指

令集合，在一些关键的程序点检查关键的操作是否会受到污点信息的影响。

第三、提供智能合约形式化验证的容器，通过数学推理逻辑和证明，检查智能合约功能正确性和安全属性，能完全覆盖代码的运行期行为，可以确保在一定范围内智能合约的绝对正确。

第 5 章. 应用场景

5.1 数据共享

区块链数据是分布式存储的一个开放数据生态，但因各方业务链系统独立建设，数据孤岛的问题依然存在，导致数据无法被其它链读取，数据无法实现共享。通过CCGP跨链智能合约对数据权限进行统一管理，数据使用者通过硬件私钥设备验证身份并对相应数据进行上传或访问，有效控制数据权限，打破区块链数据孤岛，实现同构及异构链之间的可信互通和业务协作。

5.2 联合溯源

溯源的本质是信息传递，将溯源电子证据记录到链上，溯源链的构成符合商品市场流程化的生产模式。目前，溯源链结合一物一码已经形成了通用对接解决方案，在食品、药品、保健品等防伪追溯领域成功应用。

但由于各自链的独立、分散运行，形成了溯源链、监管链、供应链金融链、电子票据、电子合同链等各种形态的单链，受限于各自联盟链的商业形态及监管要求，无法达到全域溯源主体方、参与方、监管方的协调配合，通过CCGP可以在授权接入的情况下，形成各种同构/异构链的可信数据互通，提升了区块链在溯源领域的全面协同服务价值。

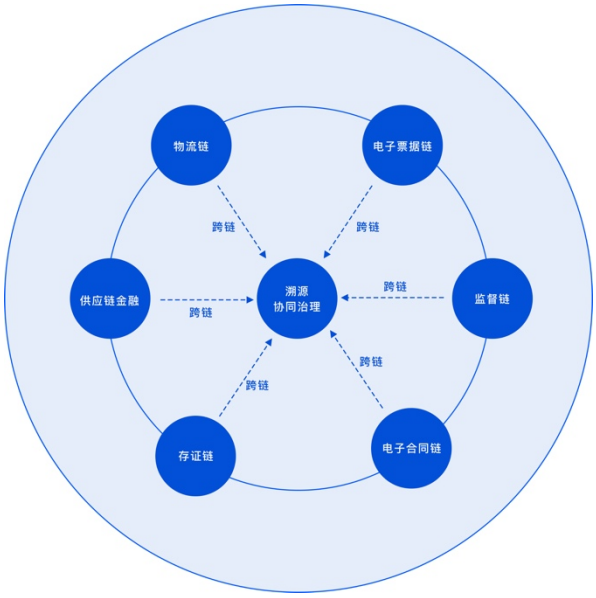

图21 联合溯源总体架构

5.3 广域存证

利用区块链技术多方参与、防篡改、可追溯的特点，解决了司法服务领域当中遇到的电子证据的取证难、存证难、认定难的问题。2020年8月5日，最高人民法院发布《关于加强著作权和与著作权有关的权利保护的意见（征求意见稿）》，《征求意见稿》提出，要大力推进案件繁简分流试点工作，大幅缩短涉及著作权和与著作权有关权利的案件审理周期。完善知识产权诉讼证据规则，支持当事人通过区块链、时间戳等方式保存、固定和提交证据，有效解决知识产权权利人举证难问题。

当前，区块链存证领域存在以企业，政府，司法机关等组织形成的区块链存证联盟链，由于业务接口，区块链基础服务等制约，不同的存证链之间无法形成数据互通，转移，验证。通过跨链治理服务，可以将不同类型的区块链存证服务，可信互通在一起，形成数据跨链校验，跨链存储的解决新思路。通过跨链授权后，可以将各类存证同构链/异构链的链上账本数据进行可信传递，保证数据的可信验证。

第 6 章. 展望

T-Sec CCGP面向产业区块链的同异构平台协作、分布式应用业务系统的连通，提供了从产业区块链技术平台协作到区块链应用业务系统协作的能力，并以“治理链”为基础，提供分布式、高安全、多阶段的跨链协议的协作方式，实践了“以链治链”的协同治理的理念。

T-Sec CCGP作为一个易用好、灵活性强、安全性高的跨链开放平台，为产业区块链构建的价值共享系统提供了“润滑剂”，让链和链协同增效。CCGP将秉持一致的开放性，与行业组织、领军企业、行业用户等一起，探索打通异构产业区块链技术和应用生态。