

基于区块链的智能服务交易跨链服务框架与通信机制

康博涵, 章宁, 朱建明

(中央财经大学信息学院, 北京 100081)

摘要: 由于不同区块链上的区块链服务间缺乏有效通信机制, 链与链之间难以形成有效互联互通。在智能服务交易过程中, 交易主客体之间不仅仅是数据资产的单项转移, 而且其服务范围扩展涵盖到更为广阔的数字资产转移场景。设计一种智能服务交易的跨链通信服务框架, 并采用基于组件式、模块化设计, 使智能服务交易主客体较为容易地接入服务框架, 实现跨链可扩展性; 提出适用于智能服务交易的三阶段跨链通信机制, 保证智能服务交易跨链生态下的原子性和一致性。

关键词: 区块链; 智能服务交易; 跨链通信; 通信机制

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021062

Research on inter-blockchain service framework and communication mechanism based on smart service transaction

KANG Bohan, ZHANG Ning, ZHU Jianming

School of Information, Central University of Finance and Economics, Beijing 100081, China

Abstract: Due to the lack of communication mechanism between inter-blockchain services, it is difficult to formulate effective interconnection between different blockchain. Under the smart services ecosystem, two parties of the transaction not only execute the single transaction of data assets, but also extend the scope of their services to cover a wider range of digital assets transfer scenarios. An inter-blockchain communication(IBC) framework for smart service transaction is designed. With component-based and modular design, it makes flexible for the subject and object application of smart service transaction to access IBC framework and thus promote inter-blockchain scalability. Finally, a three-phase inter-blockchain communication protocol for smart service transaction is proposed to ensure the atomicity and consistency of inter-blockchain ecosystem.

Keywords: blockchain, smart services ecosystem, inter-blockchain communication, communication mechanism

收稿日期: 2021-03-06; 修回日期: 2021-05-27

通信作者: 康博涵, kangbh.postgra@qq.com.

基金项目: 国家重点研发计划(2017YFB1400700)

Foundation Item: The National Key R&D Program of China (2017YFB1400700)

论文引用格式: 康博涵, 章宁, 朱建明. 基于区块链的智能服务交易跨链服务框架与通信机制[J]. 网络与信息安全学报, 2021, 7(3): 105-114.

KANG B H, ZHANG N, ZHU J M. Research on inter-blockchain service framework and communication mechanism based on smart service transaction[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 105-114.

1 引言

随着区块链底层技术的快速突破和发展,越来越多的企业积极结合其业务需求,加速融入区块链生态,并逐步在跨境支付、供应链金融、电子医疗、物联网、防伪溯源等场景展开落地与应用^[1-5]。然而,大多数的区块链应用项目是由不同的企业根据自身的需求开发,这些异构区块链网络之间无法进行互联互通,位于不同区块链上的服务缺乏通信机制,因此逐渐产生对不同区块链的跨链需求^[6]。跨链技术的关键在于保障跨链交易的真实性、有效性和原子性,现有主流跨链技术主要分为公证人机制、中继/侧链模式、哈希锁定和分布式密钥控制。表1对这4种跨链机制的实现原理和优缺点进行了简要比较。

公证人机制是一种弱中心化的跨链项目解决方案^[7]。公证人是交易双方选举一个或一组具有较高可信度的节点,对不同区块链上的交易事务进行证明和验证。公证人机制最大的优点是实现原理简单且无须复杂工作量证明,但存在中心化公证人机制的缺点。目前,有学者提出了多重签名公证人机制,在交易时随机选取一部分公证人利用密码学技术进行集体签名,从而弱化中心化风险。公证人机制的代表方案主要有 Ripple 团队提出的 Interledger 项目。Interledger 协议允许两个不同的区块链系统通过第三方“连接器”来实现双方的价值、信息的交互和资产的转移。Wang 等^[8]提出了区块链路由器的概念,该路由器可根据通信协议动态分析并传输通信请求,维护区块

链网络拓扑结构,实现链间通信。文献[9]建立了一种由数据层、网络层、共识层、契约层和应用层构成的新型体系结构,提供对多个异构区块链之间的互操作性。

中继(侧链)模式采用第三方媒介充当客户链的中继器,将跨链子交易的区块中继至相应的区块链上。中继模式与公证人模式的区别在于在该模式下,第三方媒介仅负责数据收集,而交易的确认和验证由目标链负责, Cosmos、Polkadot、BTC-Relay 等是该机制的代表项目。Cosmos^[10]提出了区块链间通信协议,通过在区块链内集成该协议,即可向目标链发送最新的区块头部信息、交易信息及其 Merkle 证明,从而达到链间通信的目的。Polkadot^[11]提供中继链作为众多异构区块链系统链接的桥梁,中继链的作用类似于一个网关,统一管理共识安全和数据交互。BTC-Relay^[12]是一种以以太坊为侧链、比特币为主链,并通过智能合约实现比特币与以太坊连接的技术。此外, Kan 等^[13]以及 Chen 等^[14]提出了交互式多区块链架构及跨链协议,该架构通过创建多链动态网络实现跨链通信,该协议可为交易提供原子性和一致性保证。叶少杰等^[15]提出了一种通用的链间消息传输协议,并实现了同时支持同构及异构区块链间交易的跨链技术示范项目平台 BitXHub; Wang 等^[16]通过在区块链上使用由心跳机制扩展的两阶段提交协议,提出一种无须集中式组件、可在多区块链上进行交易的分布式提交协议。

哈希锁定是一种实现异链间资产交换的跨链

表1 区块链跨链机制介绍
Table 1 Introduction on the inter-blockchain mechanism

跨链机制	代表项目	互操作性	优势	不足
公证人机制	Interledger	所有应用链	支持双向跨链、实现原理简单、无须复杂的工作量证明	公证人的类中心化容易造成中心化风险,存在单点失效问题
中继/侧链模式	BTC-Relay Cosmos RootStock Polkadot	所有应用链,需要接入中继链,否则只能支持跨链的单向传输	中继(侧链)模式的跨链网络更高效,能支持跨链资产变换转移、跨链合约和资产抵押	交易的确认和验证由应用链负责。需要对应用链底层扩展,开发成本较高
哈希锁定	闪电网络	交叉依赖	区块链之间通过在两条链上运行特定的智能合约,实现跨链信息交互	哈希锁定严格依赖于智能合约的执行,目前应用场景相对受限
分布式密钥控制	Fusion	所有	用户只拥有私钥就拥有资产的控制权	智能合约需要更多方面实现

技术,它要求交易的中间人和接收者在给定时间内给出正确哈希值。哈希时间锁定机制的核心思想是在规定时间内提供与哈希值对应的原内容解冻资产,代表项目为闪电网络-HTLC。文献[17]提出了一种哈希时间契约锁(HTDLC, hashed timed delylock contract)协议,通过引入违约锁,从博弈论的角度降低了单方违约的可能性,减少单方违约造成的时间成本浪费。文献[18]提出了一种基于哈希锁定的多方跨链协议,在哈希时间锁定技术的基础上,通过使用自动撮合交易算法解决多方跨链资产转移和清结算的问题。文献[19]针对 HTLC 会将支付路径公开的缺点,从隐私保护的角度对其进行改进,提出了变色龙哈希时间锁定协议。

分布式私钥控制是将数字资产的所有权和使用权分离来降低中心化的风险。分布式私钥控制的原理是将数字资产的私钥分片并发送给分布式节点进行保存,将原链上的数字资产映射到跨链上,在跨链上根据交易信息部署新的智能合约,从而创建出新的数字资产,完成数字资产的跨链转移。该技术的代表项目是 Fusion。Fusion^[20]项目旨在构建用于加密金融应用运行的基础平台,通过该平台,多种数字货币可通过智能合约自由交互,实现价值互通。

综上所述,跨链技术作为连接各区块链的桥梁,其主要应用是实现不同区块链之间的资产原子性交易、信息互通、服务互补等功能。目前,由于不同领域的区块链服务没有部署在同一个区块链底层基础设施上,且现有项目及技术对这些基础设施间仍然缺乏相互通信的能力,故存在一定的局限性。本文基于现有研究,在智能服务交易的背景下,提出了可扩展的跨链数字资产模型架构,并针对可信跨链通道的构建方式进行研究,具体如下。

(1) 针对智能交易服务的特点,设计一种交互式跨链通信核心流程和框架,该框架对跨链过程中的基础设施采用组件式、模块化设计,可通过这些模块较为容易地接入服务框架。

(2) 在跨链通信服务框架基础上,设计了适用于区块链服务跨链需求的跨链通信机制,实现数字资产转移和信息互通,杜绝了中间公证人作

恶的可能性,保障跨链交易的有效性。

(3) 设计通信报文标准协议,并提出一种基于区块链的三阶段事务提交验证机制,保证跨链交易的原子性。

2 跨链通信服务框架

为了便于区块链服务实施跨链通信,实现区块链服务的跨链需求,本文提出了跨链通信服务框架,该框架的通信整体架构是一个多层次的结构框架,采用组件式、模块化设计,降低了各功能的耦合性,如图1所示。

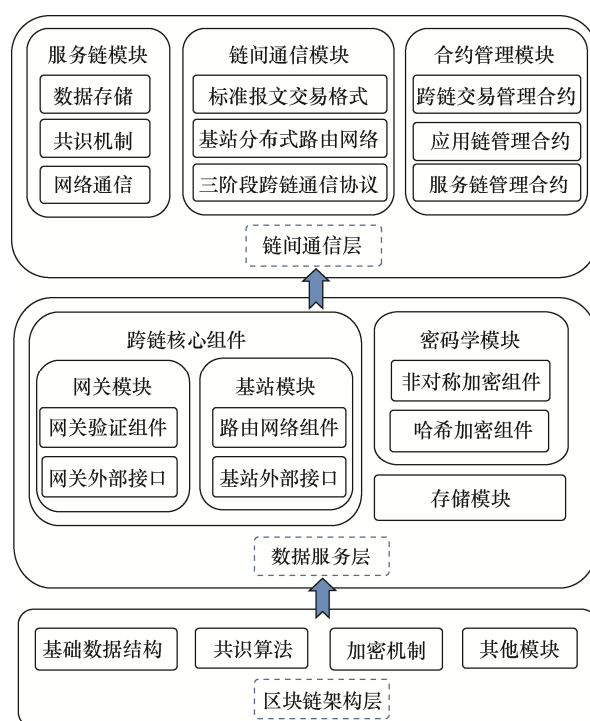


图1 跨链通信服务框架
Figure 1 Inter-blockchain communication service architecture

2.1 区块链架构层

不同的区块链底层实现机制不同,但是核心模块在于基本数据结构、共识和加密算法。跨链涉及的数据维度包含区块、交易、合约、消息等方面,智能服务交易跨链协议通过提炼通用数据结构,将跨链交易生成标准交易的报文格式。共识机制是区块链系统中各个节点达成一致的策略和方法,根据系统类型及应用场景的不同灵活选取,并封装在区块链的共识模块中;而加密算法封装在区块链加密模块中,区块链系统通过多种

密码学原理进行数据加密及隐私保护。此外,根据不同的业务需求,区块链架构层包含沙箱模块等其他模块,用于提供虚拟化隔离的安全容器,为智能合约的执行提供运行环境。

2.2 数据服务层

交易相关方实体在接入框架时,通过跨链核心设施组件、密码学组件和存储模块实现跨链功能。跨链核心设施组件包含与应用链唯一对应的网关和基站节点群模块。其中,网关模块通过PC方式连接到应用链节点,监听并对应用链节点跨链交易进行合法性和可信性验证。基站模块本质上是一种连接不同区块链系统的交互组件,各个基站通过P2P组网的方式组成跨链路由网络。每个基站会维护全网的分布式哈希路由表,记录对应网关和应用链、网关与基站间的关联关系。每个基站由权威机构进行背书,并通过集群的方式增强可信度。

密码学组件为跨链应用链提供了密码服务功能。其中,非对称加密模块提供了支持椭圆曲线加密算法的密钥管理工具,可用于快速生成公私钥对、校验签名、解密密文,可在账户生成、访问控制等功能中使用。而哈希加密组件用于标准报文在跨链基站路由间的加密传输,为数据资产交易双方提供安全加密服务。而基站和网关的注册信息、CA证书、公共参数等框架相关信息以及缓存数据存储于存储模块。

2.3 链间通信层

链间通信层包括服务链模块、链间通信模块和合约管理模块。其中服务链模块由基站和所属网关共同维护,当服务链节点接收到应用链发送的带有跨链合约调用请求后,首先对其合法性及

可信性进行验证,验证通过后将该合约调用请求存入本地内存池中,并向其他节点广播达成共识。链间通信模块主要包含标准报文交易格式、三阶段跨链通信协议和基站分布式路由网络,保证了跨链交易的真实性、有效性和原子性。合约管理模块由跨链交易管理合约、应用链管理合约和服务链管理合约等智能合约构成。

(1) 跨链交易管理合约由网关调用,用于记录跨链交易的全过程,从而实现对跨链交易的合法和可信验证。

(2) 应用链管理合约由应用链管理员和应用链节点调用,用于创建和管理应用链信息以及节点在链上的权限等。

(3) 服务链管理合约主要负责定义应用链上标准报文交易格式,以及存储跨链双方的价值转移规则。

3 面向智能服务交易跨链通信机制

考虑到跨链结构的复杂度和可扩展性,本文在链间通信采用星形拓扑结构,为所有接入该集群的区块链提供跨链服务,如图2所示。

(1) 应用链负责跨链交易的业务逻辑。

(2) 路由网关用于应用链管理以及跨链交易的可信验证与可靠路由。

(3) 基站路由网络集群担任区块链间收集信息和传播交易的角色,主要负责跨链交易智能合约收集以及转发等任务,以P2P自组网方式实现跨链交易在应用链之间的路由。

基站节点集群用于对应用链和中继链关联关系的管理以及跨链交易的可信验证与可靠路由。一般来说,不同的区块链之间没有统一的交易格式。

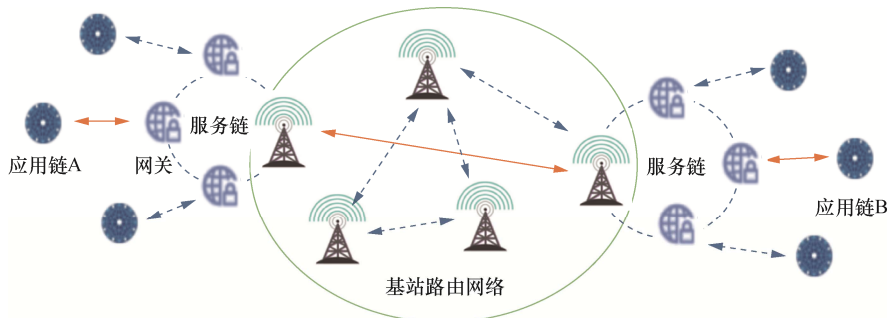


图2 链间通信层拓扑结构
Figure 2 Inter-blockchain communication layer topology

因此,本文设计一种标准交易报文格式 T ,可自适应转换为任意区块链系统发起的交易。当应用链的跨链交易发生时通过标准的跨链报文进行通信,统一标准交易报文数据结构如表2所示。

表2 标准交易报文数据结构
Table 2 Standard trading packet data structure

结构参数	内容说明
From	发起来源链 ID
To	目的链 ID
Index	跨链交易索引
Timestamp	跨链事件发生的时间戳
Acknowledgement	目的链确认信息
Content	交易具体内容
Proof	跨链交易证明
Extra	其他自定义字段

From 和 To 字段分别代表主客体来源链和目的链的 ID,在应用链向基站注册时生成。

Index 是跨链交易的索引,跨链交易按其来源链 ID 分别进行排序编码。

Timestamp 字段是跨链交易的时间标识。

Acknowledgement 字段为布尔类型,用于目的链验证确认收到交易信息。

Content 字段为跨链调用的内容编码,支持哈希加密,可由应用链的业务需求确定。

Proof 字段存储了跨链交易合法性证明,为网关和基站跨链验证引擎提供具体的验证信息。Proof 字段内容根据来源链的不同而不同,具体验证规则可通过动态加载的方式注册到网关验证引擎。

扩展字段 Extra 可根据应用链的业务需求进行自定义。

本文对来源链 A 中的交易地址 A_1 到目的链 B 中地址 B_1 的跨链交易 Transfer 用合约函数义为

$$\text{Transfer}(A_1, B_1, \text{value})$$

本文定义 T_A 和 T_B 分别是应用链 A 和 B 对应的服务链内交易,并通过标准跨链交易为中介载体进行跨链传输。跨链交易的通信过程将应用链 A 的交易通过服务链的 Package 过程封装为标准跨链交易 T ,再通过对目的服务链的 Unpackage

过程将 T 转换到应用链 B 中。

根据跨链通信模型,一次完整的跨链交易 T 的交易过程如下。

(1) 交易主体向应用链 A 发送指令交易函数 Transfer。

(2) 网关在监听到跨链事件后,通过 WASM 验证引擎对交易进行真实性验证和合法性验证。验证通过后,构建 Merkle 证明及签名背书,并构造 proof 字段。然后,由网关封装成标准跨链交易 T ,经由服务链节点合法性验证并参与共识后,在服务链上构建跨链交易 T 的记录,并存储 Merkle 证明。

(3) 当对应基站监听到服务链的共识跨链事件,将经哈希加密的标准报文 T 通过分布式哈希表中继传输到对应目的基站,验证其数字签名,并发送目的服务链节点进行共识。

(4) 目的链网关监听到跨链事件后对 T 进行合法性验证,之后构建 Merkle 证明并用其私钥签名,发送至应用链 B,服务链节点经合法性验证并共识后,更新跨链交易 T 的状态并存储 T 的 Merkle 证明,随后向来源链发送 ACK 消息进行三阶段交易原子性确认协议。

4 跨链通信服务协议

在智能服务跨链交易的应用场景中,来源链需要确认资产交易是否到达目的链。此外,两个涉及交易的应用链在完成跨链交易事务后必须具备相同的记账结果。为了保证智能服务交易跨链交易过程的原子性和一致性,本文在文献[13]提出的三阶段跨链通信协议基础上,进一步适应智能服务交易跨链通信机制的需要,并对该协议添加可信性证明机制,以满足交易主客体之间的安全性需求,使交易结果保持一致。其中,路由网关充当三阶段协议中的协调者和验证者角色,而基站节点负责跨链交易协议下消息中继传输的功能。从 Prepare 阶段起,网关向全体参与跨链事务的资源发起阶段性请求,如果任意阶段消息返回或验证失败,路由网关就会发起交易的回滚请求(Roll back),进行非法交易的回滚操作,通过这种方式可以在任意阶段做出中止交易的确认请求。协议过程描述如图3所示。

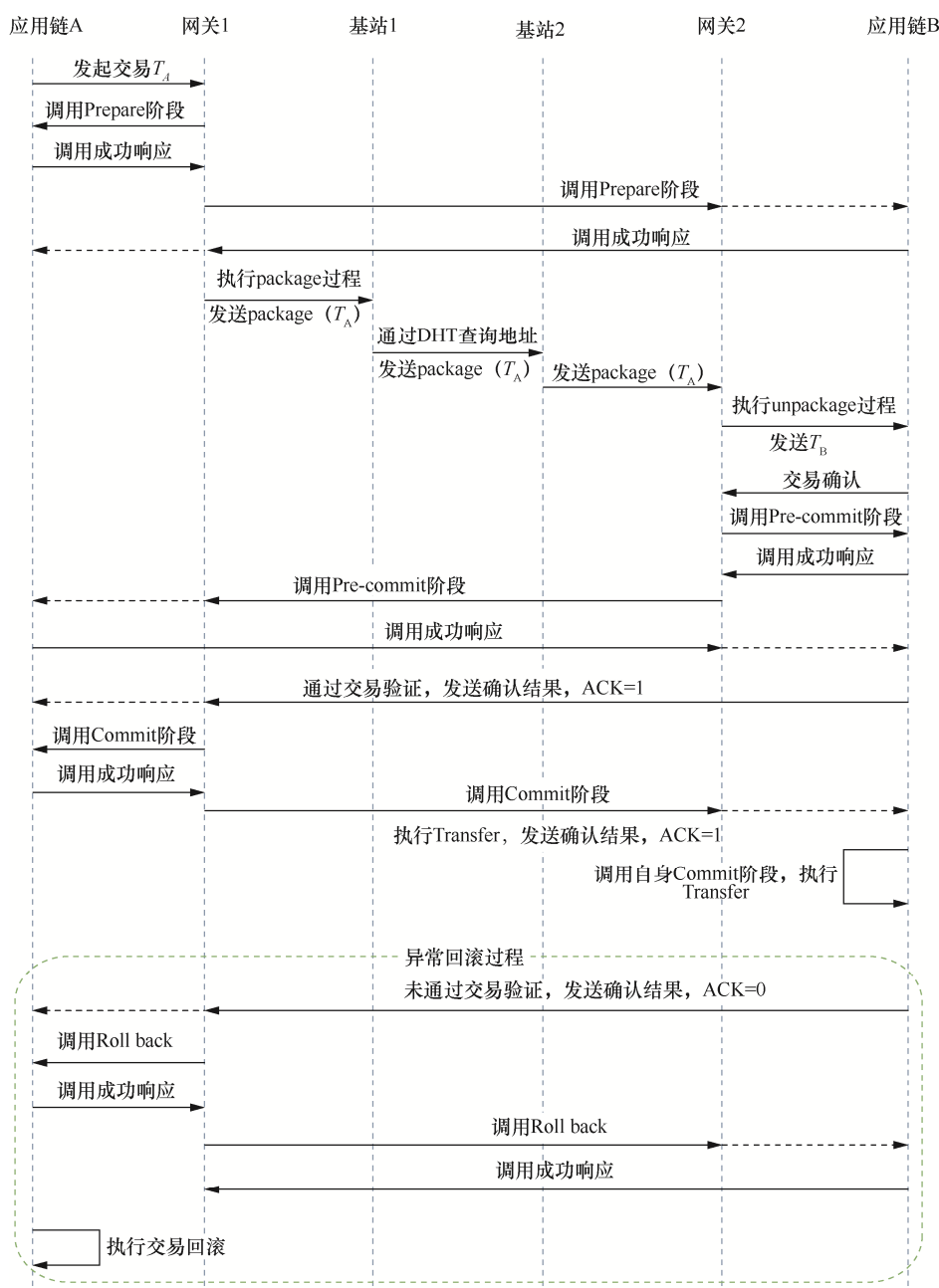


图 3 跨链交易成功执行步骤

Figure 3 Process of transaction successfully committed

(1) 应用链 A 发起跨链资产交易 T_A ，并向网关请求调用 Prepare 阶段，之后 T_A 被转发到与应用链 A 耦合的网关 1 节点。

(2) 网关 1 经可信和合法验证后, 将 T_A 通过 **Package** 过程转换成标准交易报文 T , 在服务链参与共识, 并判断目的链地址是否在其管理的应用链地址列表。如果查询到目的链的注册证书位于基站管理地址, 则执行 **Unpackage** 过程将 T 转换

为 T_B ，经由网关发送到应用链 B 中，否则通过基站分布式哈希表（DHT）的方式进行寻址，并发送到目的链所关联的基站，之后执行验证、共识和 Unpackage 过程。

(3) 目的链 B 在接收到报文 T_B 后进入 Pre-commit 阶段, 对数字签名等进行验证, 确认交易结果, 并将确认结果 ACK=1 经由网关和中继基站发送给应用链 A。

(4) 当应用链 A 收到 $ACK=1$ 的确认消息后, 申请调用进入自身 Commit 阶段, 执行 Transfer, 将交易 T 写入自身的本地账本中, 并将确认消息 $ACK=1$ 发送给应用链 B。

(5) 应用链 B 在收到 $ACK=1$ 确认消息后, 进入自身 Commit 阶段并执行 Transfer 合约, 交易 T 的最终结果被记录到应用链 B 的本地账本。

(6) 若应用链 B 在 Prepare、Pre-commit 和 Commit 任意阶段多次未按时接收到消息响应或交易验证失败, 则通过网关和基站路由向应用链

A 发送 $ACK=0$ 。

(7) 应用链 A 在收到 $ACK=0$ 消息后进行跨链交易 T 的回滚操作。

所有主客体应用链之间的交易通信是基于点对点传输的, 然而基于点对点跨链交易事务的报文传输会受到数据包丢失、数据传输错误或其他网络问题的干扰。为避免网络不稳定导致报文传输交易失败, 本文设计了一种跨链交易超时重传策略, 如图 4 所示。

(1) 应用链 A 在完成 Prepare 阶段和 Package

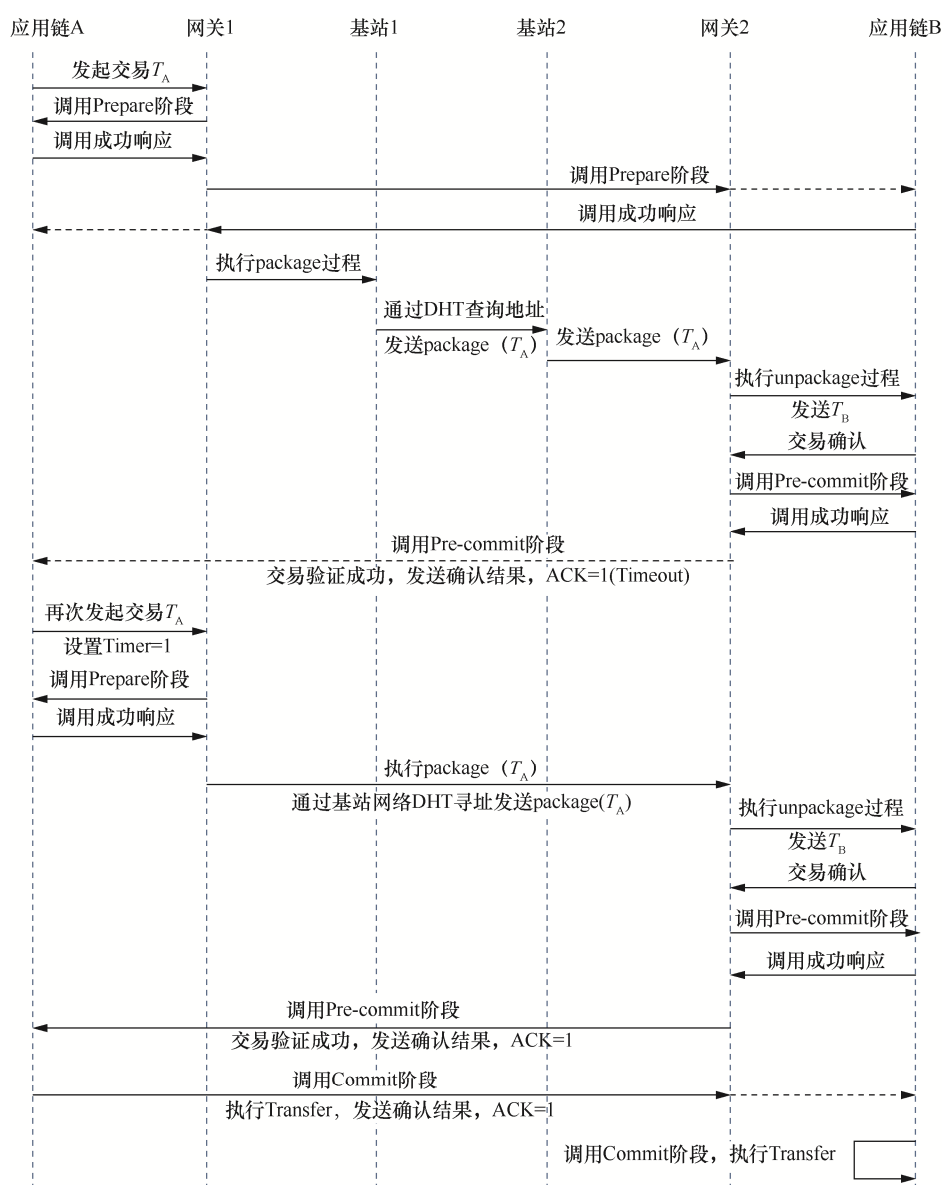


图 4 跨链交易超时重传步骤 (Timer=1)
Figure 4 Process of transaction retransmission (Timer=1)

过程后, 设置一个 Timer。

(2) 当 Timer 倒计时至 0, 如果应用链 A 仍然没有收到目的链 B 的 ACK 消息响应, 则应用链 A 重新发送跨链交易 T 并重置 Timer。

(3) 应用链 A 最多重置三次 Timer, 如果三次始终没有收到目的链 ACK 消息响应, 则应用链 A 执行跨链交易 T 的非法交易回滚操作, 否则进入 Commit 阶段。

5 安全性分析

5.1 智能服务交易跨链协议的可信性分析

区块链重要的安全假设是“每个参与节点都存在作恶风险”, 而在此假设下通过密码学和共识算法构建区块链分布式可信环境。但在跨链的生态环境下, 单个区块链内部的可信环境无法被其他区块链所信任, 因此需要引入额外的可信证明来实现智能服务跨链的信息交互。智能服务的跨链交易在 proof 字段中添加了 Merkle 相关证明, 用于对应用链传输交易和回执的可信验证。本文为网关设计了一种高效可插拔的验证引擎, 通过智能合约的方式管理多种验证规则, 对不同应用链的交易进行合法和可信性检验。验证引擎工作流程分为 3 个步骤。

(1) 协议解析: 协议解析是验证引擎内部对跨链交易的解析。由于所有跨链交易都遵循跨链标准报文协议, 该步骤可以解析出交易信息和验证信息作为后续验证引擎的输入。

(2) 类型匹配: 类型匹配是验证引擎根据上述协议解析步骤解析出来的来源链类型, 匹配对应的验证规则脚本。

(3) 规则执行: 规则执行主要通过 WASM 虚拟机动态加载验证规则脚本, 对跨链交易的 Proof 字段进行校验, 保证交易的可信性。

智能服务交易的跨链协议采用区块头同步设计, 将节点待跨链同步的区块头信息存储于智能合约。在应用链接入服务链之前, 需要进行验证规则的编写和注册, 并由服务链审核后部署到网关验证引擎。当进行跨链交互时调用跨链验证合约的接口, 状态信息同步者将证明同步给目的链网关后, 目的链节点将继续处理交易业务信息, 如图 5 所示。

可靠性交互流程具体流程如下。

(1) 来源链的跨链管理合约会为每笔跨链交易分配一个自增 ID, 并将跨链交易放入 Merkle Tree, 而 Merkle Root 会被放入待跨链区块的区块头中, 完成后将该 ID 和区块高度等信息通过

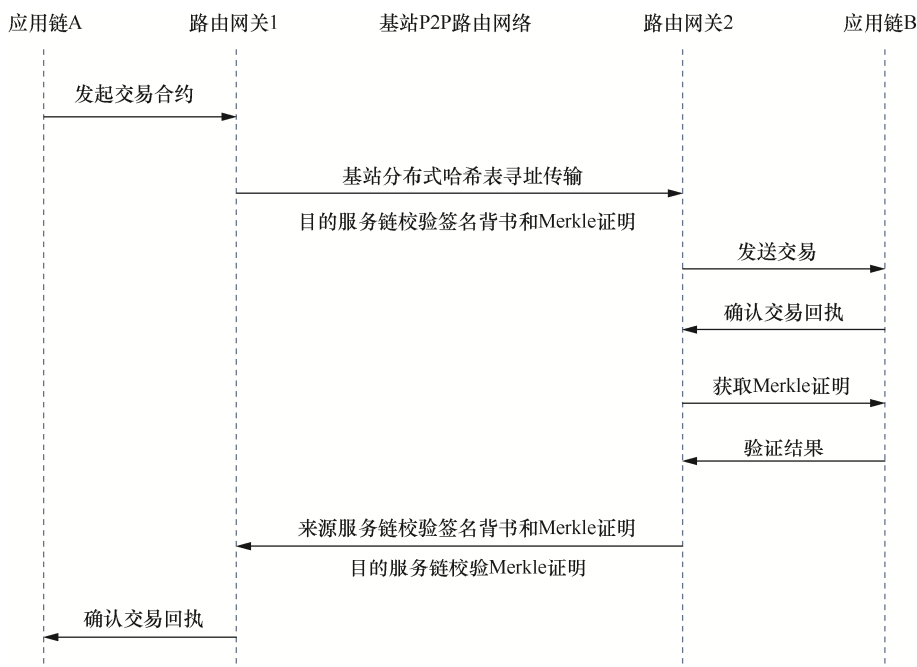


图5 链间交易可靠性交互流程
Figure 5 Inter-blockchain transaction reliability interaction

package 操作生成标准报文推送至对应网关。

(2) 服务链上基站负责监听这些跨链事件，当监听到一笔跨链交易时，网关节点根据 ID 和区块高度到来源链上获取 Merkle 证明，检验报文的 Proof 字段，并将 Merkle 证明和自身签名提交到目的链。

(3) 目标链接收到该 Merkle 证明和网关的检验背书，并将标准报文进行 Unpackage 操作，获取对应的区块头，得到 Merkle root 并验证在来源链上已完成的跨链交易的合法性，然后根据跨链交易的参数，跨合约调用目标链上的智能合约，完成目标链上业务信息的处理。

5.2 智能服务交易跨链协议的可扩展性证明

对于区块链的可扩展性，有两个重要的衡量指标：交易的吞吐量（区块链单位时间处理交易的数量）和交易的确认时延（交易被打包到区块中并被确认不可逆的时间）。智能服务交易跨链平台架构的可扩展性表现为随着接入应用链数量的增加以及交易的增多而导致吞吐量和时延的变化情况。本文部署两条 Hyperledger fabric 区块链节点集群分别作为主客体的来源链和目的链，并对每条应用链部署一个跨链网关。通过不断提高发起主客体应用链间资产交易来测试上述性能。不同区块链集群的峰值吞吐量如图 6 所示，不同数量区块链集群的交易确认时延如表 3 所示。

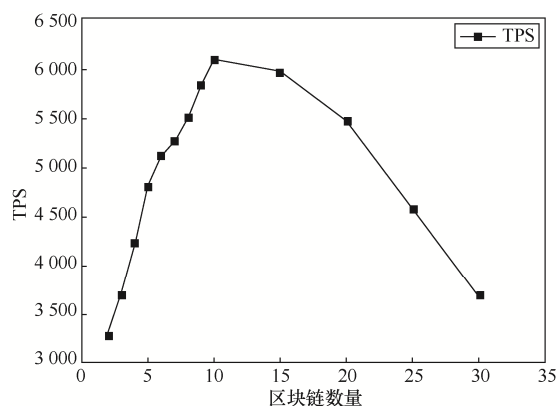


图 6 不同区块链集群的峰值吞吐量
Figure 6 Peak throughput of different IBC clusters

可以看出，当系统部署应用链大于 10 条时，智能服务交易跨链通信架构的吞吐量性能由峰值 6 100 TPS 显著下降，其原因是在大规模集群应用链上的交易测试采用了基于 Hyperledger fabric 区

块链内置的 kafka 共识算法，从而导致大量性能开销。

随着应用链集群的增多，智能服务跨链交易的确认时延显著提升。原因在于跨链模型中随着各个不同异构或同构应用链的接入，节点的网络拓扑结构会愈发复杂，其中主要体现在对不同交易的 proof 字段检验的开销。此外，随着加入的应用链不断增多，系统对基站分布式网络传输的稳定性提出了更高的要求。

表 3 不同数量区块链集群的交易确认时延
Table 3 Transaction confirmation delay for different number of blockchain clusters

接入区块链数量	跨链交易确认时延/ms
2	35
5	106
10	133
15	328
20	621

5.3 智能服务交易跨链协议的真实性分析

真实性指互不信任的区块链间构建去信任的跨链子交易。跨链模型的跨链交易管理合约由基站和网关调用，用于记录跨链交易的全过程，从而实现对跨链交易的可信验证。当服务链在接收到由网关发送的合约调用请求时，服务链节点首先对网关的身份及其提交的跨链子交易真实性进行验证，之后，根据子交易的内容和当前其涉及的跨链交易状态对该子交易的合法性进行二次验证，验证通过后广播至其他服务链节点做相同的验证操作并等待共识，共识通过后即可根据合约调用请求修改状态机的状态。

6 结束语

本文提出了一种智能服务交易跨链通信核心流程和框架，并在跨链通信服务框架基础上，设计了适用于区块链服务跨链需求的跨链通信机制，提出了面向区块链服务的跨链通信服务框架；研究和设计了跨链通信服务框架中各模块的功能和 workflows，设计了跨链用户与跨链通信服务框架的基本交互逻辑；通过区块链的通用跨链协议和三阶段事务提交验证机制，保障跨链交易的可信性、有效性和原子性。未来研究可对服务链共

识机制等进行优化以达到提高服务链的吞吐量的目的,以及对中继基站的功能、模块、激励措施等进行进一步的研究。

参考文献:

- [1] AHLUWALIA S, MAHT R V, GUERRERO M D. Blockchain technology and startup financing: a transaction cost economics perspective[J]. Technological Forecasting and Social Change, 2020, (151): 1-6.
- [2] SUN B L, LYU Z H, LI Q. Obstetrics nursing and medical health system based on blockchain technology[J]. Journal of Healthcare Engineering, 2021(2):1-11.
- [3] LI X H, WANG D B, LI M L. Convenience analysis of sustainable E-agriculture based on blockchain technology[J]. Journal of Cleaner Production, 2020(271).
- [4] 谭海波, 周桐, 赵赫, 等. 基于区块链的档案数据保护与共享方法[J]. 软件学报, 2019,30(9):2620-2635.
TAN H B, ZHOU T, ZHAO H, et al. Archival data protection and sharing method based on blockchain[J]. Journal of Software, 2019, 30(9): 2620-2635.
- [5] 何正源, 段田田, 张颖, 等. 物联网中区块链技术的应用与挑战[J]. 应用科学学报, 2020, 38(1): 22-33.
HE Z Y, DUAN T T, ZHANG Y, et al. Blockchain in internet of things: application and challenges[J]. Journal of Applied Sciences, 2020, 38(1): 22-33.
- [6] 李芳, 李卓然, 赵赫. 区块链跨链技术进展研究[J]. 软件学报, 2019, 30(6): 1649-1660.
LI F, LI Z R, ZHAO H. Research on the progress in cross-chain technology of blockchains[J]. Journal of Software, 2019, 30(6): 1649-1660.
- [7] 刘海, 李兴华, 雒彬, 等. 基于区块链的分布式 K 匿名位置隐私保护方案[J]. 计算机学报, 2019(5): 942-960.
LIU H, LI X H, LUO B, et al. Distributed K-anonymity location privacy protection scheme based on blockchain[J]. Chinese Journal of Computers, 2019(5): 942-960.
- [8] WANG H, CEN Y, LI X. Blockchain router: a cross-chain communication protocol[C]//Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications. 2017.
- [9] JIN H, DAI X. Towards a novel architecture for enabling interoperability amongst multiple blockchains[C]//IEEE 38th International Conference on Distributed Computing Systems. 2018.
- [10] KWON J, BUCHMAN E. A network of distributed ledgers cosmos[EB].
- [11] WOOD G. Polkadot: vision for a heterogeneous multi-chain framework[EB].
- [12] CONSENSYS. BTC relay's documentation[EB].
- [13] KAN L, WEI Y, MUHAMMAD A H, et al. A multiple blockchains architecture on inter-blockchain communication[C]//2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C). 2018: 139-145.
- [14] CHEN Z, ZHUO Y U, DUAN Z, et al. Inter-blockchain communication[J]. DEStech Transactions on Computer Science and Engineering, 2017 (cst).
- [15] 叶少杰, 汪小益, 徐才巢, 等. BitXHub: 基于侧链中继的异构区块链互操作平台[J]. 计算机科学, 2020, 47(6): 294-302.
YE S J, WANG X Y, XU C C, et al. BitXHub: side-relay chain based heterogeneous blockchain interoperable platform[J]. Computer Science, 2020, 47(6): 294-302.
- [16] WANG X, TAWOSE O T, YAN F, et al. Distributed nonblocking commit protocols for many-party cross-blockchain transactions[J]. arXiv preprint arXiv: 2001.01174, 2020.
- [17] 魏昂. 一种改进的区块链跨链技术[J]. 网络空间安全, 2019, 10(6): 40-45.
WEI A. An improved cross-chain technology of blockchain[J]. Cyberspace Security, 2019, 10(6): 40-45.
- [18] 张诗童, 秦波, 郑海彬. 基于哈希锁定的多方跨链协议研究[J]. 网络空间安全, 2018, 9(11): 57-62.
ZHANG S T, QIN B, ZHENG H B. Research on the protocol of multiple cross-chains based on the hash lock[J]. Cyberspace Security, 2018, 9(11): 57-62.
- [19] YU B, KERMANSHAH S K, SAKZAD A, et al. Chameleon Hash time-lock contract for privacy preserving payment channel networks[C]//2019 International Conference on Provable Security. 2019: 303-318.
- [20] Fusion[EB].

[作者简介]



康博涵(1993-), 男, 河北石家庄人, 中央财经大学博士生, 主要研究方向为区块链应用、数字经济。



章宁(1975-), 女, 江西临川人, 中央财经大学教授、博士生导师, 主要研究方向为金融科技、管理信息系统。



朱建明(1965-), 男, 山西太原人, 中央财经大学教授、博士生导师, 主要研究方向为信息安全、区块链技术。