

文章编号: 1000-5641(2020)05-0044-12

一种面向双中台双链架构的内生性 数据安全交互协议研究

刘 峰^{1,2}, 杨 杰², 李志斌³, 齐佳音^{2,4}

(1. 华东师范大学 计算机科学与技术学院, 上海 200062; 2. 上海对外经贸大学 人工智能与变革
管理研究院, 上海 200336; 3. 华东师范大学 数据科学与工程学院, 上海 200062;
4. 可信分布式计算与服务教育部重点实验室, 北京 100086)

摘要: 自“数据+业务”的双中台架构被提出以来, 中台间数据进行安全交互的效能显得尤为重要. 基于此, 本研究提出了一种高效的交互式协议, 在借助区块链双链结构保证数据安全可信的情况下, 改善了内生性数据在中台间交互效率低的问题. 对新协议中核心的门限签名技术进行实验模拟的结果表明新协议在链下签名、链上验签过程中比传统单一链上签名及验签的方法节省了 42.1% 的时间成本. 新协议对中台融合区块链技术、加快中台与区块链的广泛实践均具有积极推动作用.

关键词: 双中台双链架构; 高效数据交互协议; 链下门限签名; 链上验证签名; 区块链

中图分类号: TP301 **文献标志码:** A **DOI:** 10.3969/j.issn.1000-5641.202091014

Research on an endogenous data interaction protocol for the dual-middle platform and dual-chain architecture

LIU Feng^{1,2}, YANG Jie², LI Zhibin³, QI Jiayin^{2,4}

(1. School of Computer Science and Technology, East China Normal University, Shanghai 200062, China;
2. Institute of Artificial Intelligence and Change Management, Shanghai University of International
Business and Economics, Shanghai 200336, China; 3. School of Data Science and Engineering,
East China Normal University, Shanghai 200062, China; 4. Key Laboratory of Trusted
Distributed Computing and Services, Ministry of Education, Beijing 100086, China)

Abstract: Since dual-middle platform architecture of “data and business” was first proposed, the efficiency of secure data interaction between middle platforms has become particularly important. This paper proposes an efficient interaction protocol, while ensuring data security and credibility with the help of a blockchain dual-chain structure, to optimize the efficiency of endogenous data interaction between middle platforms. By extracting the core threshold signature technology in the new protocol, the simulation experiment showed that the protocol reduced 42.1% of the overhead time used in the off-chain signature and on-chain verification processes compared with the method for traditional single signature and on-chain verification. The new protocol will have a positive impact on the integration of blockchain technology in the middle platform and on accelerating the overall adoption of the middle platform and blockchain.

收稿日期: 2020-08-14

基金项目: 国家自然科学基金(72042004)

第一作者: 刘 峰, 男, 博士研究生, 研究方向为区块链、密码学、数据科学. E-mail: lsttoy@163.com

通信作者: 齐佳音, 女, 教授, 博士生导师, 研究方向为前沿技术与变革管理. E-mail: ai@suibe.edu.cn

Keywords: dual-middle platform and dual-chain architecture; efficient data exchange protocol; off-chain threshold signature; on-chain verification signature; blockchain

0 引言

传统的数据中台主要服务于数据的分层与属性分离,具有沉淀公共数据的能力。数据中台是通过数据技术对海量数据进行采集、计算、存储、加工,同时统一标准和口径的一种共享平台。其最早由阿里巴巴于2016年的研究报告中提出,目的是帮助实现全局数据规范,力图将技术平台开发的功能充分反哺到前端应用^[1]。阿里巴巴数据中台出现的缘由则是来源于其内部众多业务部门千变万化的数据需求和高速时效性的要求,既要满足多个业务前台的数据需求,同时还要应对大规模数据的线性可扩展问题以及复杂活动场景业务系统的解耦问题等^[2]。不过,数据中台的概念目前仍过于宽泛,业界亦无行业性标准。在国内科技公司竞相展开大中台规划的时候,阿里巴巴首席信息官张建锋近些年则在不同场合提出了业务中台的架构思想。所谓的业务中台是指所有应用系统都必须与之建立联系,以便更好地实现企业核心业务运行机制的一种整合型体系系统。张考虑使用业务中台与数据中台融合创新的新思路来进一步细化中台职能。但是,数据中台和业务中台融合过程中存在的突出问题是数据交互的效能问题。在中台间多股业务流和数据流交互传输时,很难明晰出一条完整的业务与数据处理过程。内生性的业务信息与数据信息的杂糅,导致业务流的溯源、数据流的调度变得烦琐,数据交互的安全性也面临着一定的挑战。因此,如何确保在安全情况下提升中台间内生性数据交互效能以推动中台建设是亟待研究的问题。

针对上述问题,本研究使用区块链技术来对交互的数据进行拆分。区块链技术作为一种点对点的新兴计算机技术,可以在解决业务溯源困难、数据调度粗略问题方面提供可能途径。借助区块链技术特性,一方面赋能“数据+业务”的双中台系统在数据安全流转和数据安全存储方面的隐私保护;另一方面借助共识机制和经济模型,融合区块链生态的资源来对实际落地场景进行技术融合创新。区块链技术融于双中台,但并不会侵入相关中台业务,而是类似作为中台系统的底层技术进行赋能,避免了区块链技术直接对海量数据进行处理的低效率问题。利用区块链公开透明、难被篡改等优势,能够对已经处理过的有价值数据进行流转、存储及追溯,从而最终服务于数据交互效能的提升。

本研究根据中台中交互数据源的不同,将业务流信息和数据流信息放置于基于区块链的业务链和数据链上分别进行存储,进而提出了一种面向双中台双链架构的内生性数据安全交互协议。通过该协议,核心数据信息通过集合中台中一定数量的信息主体对上链数据信息进行授权,将合法信息批量传入指定区块链。同时,抽离协议中核心的门限签名算法构造内生性数据交互流转的模型。通过实验,分析算法在进行数据交互时的时间开销,并与传统的链上单一签名、验签进行比较,证实了该协议在改善数据交互效能上具有一定的优势。

1 研究基础

1.1 数据中台现状

不少学者为推动中台的发展做了相关的研究,概括而言,目前的数据中台的阶段模式可以分为以下三种。

第一种是阿里巴巴最初提出的数据中台,主要是为了在“大中台,小前台”的业务战略下进行数据化的实践^[2],通过划分不同业务边界然后进行业务建模,进而指导系统的服务化建设。在延续阿里巴巴提出的数据中台战略思想的基础上,邓立君提出紧跟大数据时代的发展潮流,通过融合数据中台到大

数据中心的建设中, 实现对所有业务进行数据化处理, 以充分发挥数据资产价值^[3].

第二种是业务中台. 根据业务需求的不同, 划分不同业务边界然后进行业务建模, 进而指导系统的服务化建设. 对于业务中台的作用, 宫志奇认为业务中台能够解决效率问题, 同时也能降低业务创新成本^[4]. 而赵冠东等学者则是考虑基于业务中台技术对全渠道运营支撑平台架构进行改良设计, 主要包括运营活动、运营渠道管理以及监督预警, 并研究了部署方式和面向电力营销的运营支撑平台的业务内容^[5].

第三种是碎片化中台. 在前两种数据中台的基础之上, 根据业务或职能进行更细粒度的拆分, 使得中台碎片化, 以降低成本, 进一步提高组织效率. 在此类中台实践中, 付威认为数据中台遵循高度集中化与可复用原则, 可在中台基础上将服务组件快速封装起来, 提供给前台便利使用^[6].

传统数据中台功能过于集中化, 而在真实的业务场景下, 系统往往需要通过不同的业务服务来获取业务所需要的数据. 这种方式即便考虑用分布式系统架构来实现传统的数据中台相关功能, 技术上仍然存在缓存穿透、造成雪崩效应的问题. 为解决这一痛点, 通常的做法是进行数据治理, 可以实现更高效地提升高并发业务场景下的计算和存储能力^[7-8]. 但考虑到业务的需求分析会随着不同时间点动态变化, 如果不能对新业务进行及时处理^[9], 也无法做到在技术上根据需求的特性进行持续功能迭代和技术更替, 那么数据治理的效益将会大打折扣. 因此“数据+业务”形式的双中台架构逐渐进入产业界中.

1.2 “数据+业务”双中台

典型的“数据+业务”双中台架构将数据处理与业务服务按照逻辑顺序及处理对象属性进行并列设计, 使得业务上的需求分析能够及时得到反馈, 有助于缓解现有数据平台中单一数据中台业务冗余的技术痛点, 达到有效进行数据治理的目的. 同时业务中台的剥离, 还有助于一部分业务信息能提前进行预处理, 从而提升业务处理效能. 具有普适性的“数据+业务”双中台架构如图 1 所示.

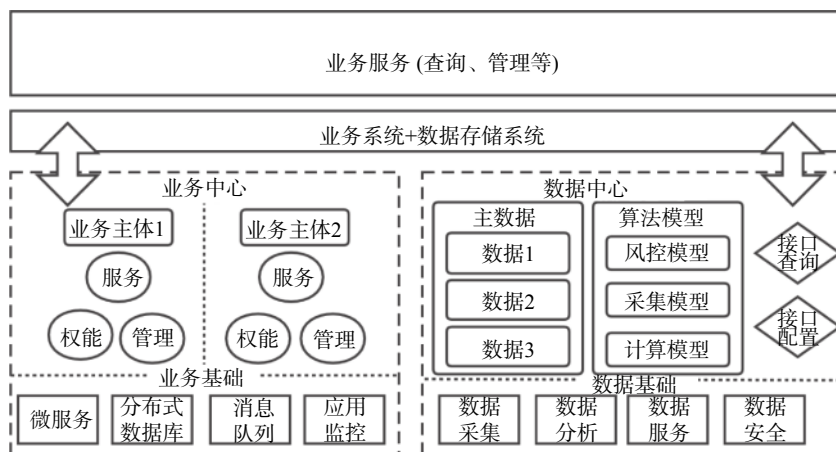


图 1 双中台架构图

Fig. 1 Architectural diagram of dual-middle platform

从图 1 的左半部分业务中台可以看出, 业务中台的基础件是由业务中的微服务平台、分布式数据库、消息队列和应用监控组成的, 上层则根据业务主体的不同, 分配不同的服务、权能和管理措施. 右半部分数据中台的基础件是由数据采集、数据分析、数据服务和数据安全四个部分组成, 数据中台中会依照不同的算法模型对不同的数据进行不同的处理. 在风险控制模型中, 需要对主数据的安全性、质量进行评估分析; 在采集模型中, 需要对上传的数据进行归类, 收集整合同类业务数据进行后续处理; 对于计算模型, 主要是根据业务需要提取数据中的关键信息进行分析计算, 然后给出对应的处理

结果.此外,数据中台还会向外提供数据查询的接口并给出相应的数据接口配置,方便根据服务需求进行调整,然后调用.

在这种双中台架构下,进行业务分析时,使用业务中台进行处理;进行数据分析时,则使用数据中台进行处理,从而减少业务和数据的耦合度.与此同时两者还能相辅相成、互相改进,形成增强闭环,并进一步降低各中台中信息的冗余,提升一定的计算效能.

1.3 基于区块链技术的双中台架构

在数据中台逐渐丰富和完善的同时,区块链技术也在走向成熟.例如,毕娅等人就提出了一种用户信息链和交易链的双链结构,在保证用户隐私的同时,将业务信息与交易数据进行拆分,减少了节点记录信息的冗余量^[10].再如,Gai等提出了用于融合区块链和数据中台以创造附加价值的概念模型^[11].Li等人也给出了一种使用区块链技术来实现整个数据生命周期中的数据跟踪的方法^[12].

鉴于上述先行研究,在双中台的基础上,为了在数据安全可信的情况下更好地对数据信息和业务记录进行管理,本研究也引入了基于区块链技术的双链架构^[10].根据具体业务和数据读取的需要,将具有不同共识机制、不同经济模型、不同交易处理能力的区块链进行组合,以便借助不同的区块链生态力量搭建最符合实际场景的业务体系.具体的双链架构设计如图2所示.

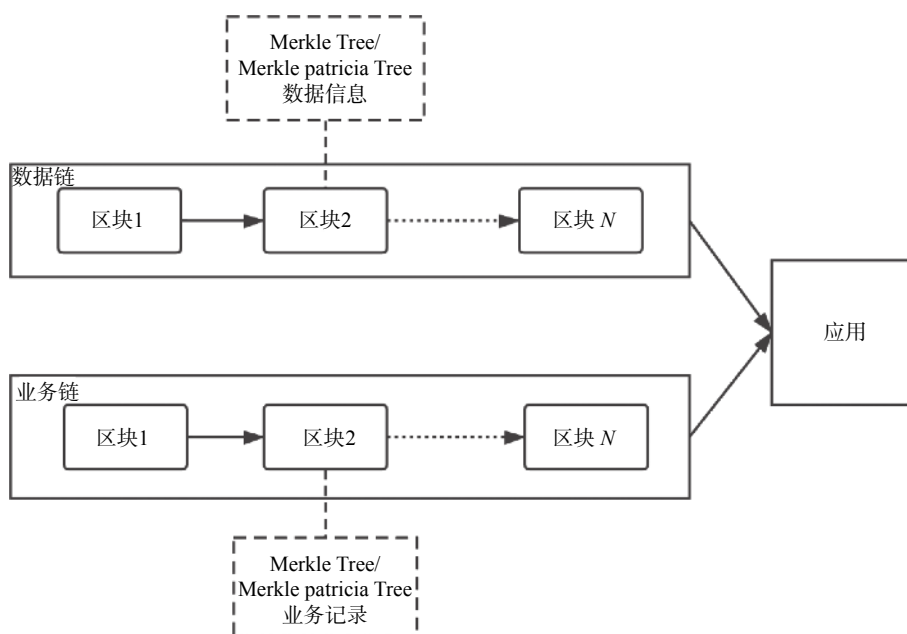


图2 双链架构图

Fig. 2 Architectural diagram of dual-chain

双链架构依据数据链和业务链进行拆分,并最终服务于一个应用中处理.数据链的区块中存储的是数据信息,业务链的区块中存储的是业务记录.根据业务和数据特性,架构中数据链是作为私有链,而业务链可以是公有链,也可以是联盟链.然后根据数据、业务记录的具体信息决定是采用默克尔树(Merkle Tree)结构存储的区块链还是用默克尔帕特里夏树(Merkle Patricia Tree)结构存储的区块链.同时对于双链架构并不限定数量为两条链,而有可能是以数据类型和业务类型所区分的两种链.每一种链均可以由具体的去中心化应用(Dapp)或调用服务来进行协同通信.

这样的实现方式会在内生性数据交互上有以下三个方面的好处:1)链上的任意用户节点可以在不知道隐私数据信息的情况下查看大致的业务处理情况,这样就在保证数据安全的同时,也保证了业

务记录的真实可信; 2) 将业务记录和数据信息拆分开来, 相比单链处理, 同一时刻能够减少大部分节点记账信息的冗余, 一定程度上提高了系统的吞吐量性能; 3) 方便系统运维和管理, 能够在逻辑上进行业务的平滑扩展.

结合上述的基础知识, 本文给出双中台双链架构下的数据交互过程, 如图 3 所示. 首先, 将某个数据源输入数据中台, 由数据中台采集数据后, 对数据源中的信息进行安全分析. 然后经过数据中台周转, 将信息存入数据链. 与此同时, 抽离出数据源的业务数据交由业务中台进行处理判断. 对不同主体进行不同的业务处理, 然后将其传入业务链中进行保存, 并根据业务需求输出结果反馈, 即实施业务服务.

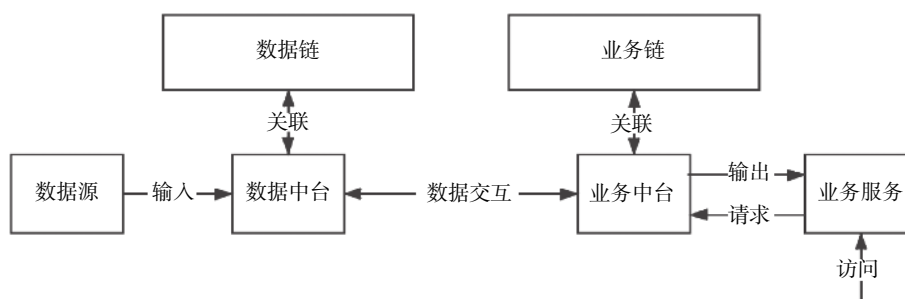


图 3 双中台双链交互流程

Fig. 3 Dual-middle platform and dual-chain interactive process

如果业务主体需要进行相关服务, 那么需要经过业务中台的业务服务进行访问, 由业务服务反馈给业务中台后, 向数据中台请求相关数据的调用, 并记录此次业务数据到业务链. 数据中台收到请求后进行合法确认, 然后调用数据链上的内容进行返回, 最终将内容反馈给业务主体. 因此, 双中台的架构设计既有效地提高了数据在业务链路分片的准确度和效率, 同时减少了数据耦合, 有利于在未来业务中对数据集进行预分类. 而且, 在以双中台架构为核心的基础上融入双链架构, 对比单一区块链结构更有效地利用了解耦思想来对上链信息进行合理区分. 在不使用效率和性能相对低下的跨链交互技术的同时, 还能够最大限度地减少区块链数据的并发数据量, 提高吞吐量, 极大地提高了双中台双链系统的整体效能.

但是, 在充分利用双中台双链架构的技术优势之时一个无法回避的问题也随之产生, 即为了充分利用区块链公开透明、全程加密、安全追溯的优势, 在双中台与双链之间做签名和验签时会面临低效的问题, 因此设计一个相对高效的交互协议来提升交互效率就显得尤为重要.

2 一种面向双中台双链架构的内生性数据交互协议

针对以双中台为核心的分布式系统和去中心化区块链系统间的数据协同中的效能问题提出以下的协议. 如图 4 所示.

结合图 4, 以业务中台和业务链间数据交互为例, 研究中的协议核心部分按照舒普 (Shoup) 门限签名算法^[13]来对业务主体传输的业务记录进行授权后上链. 一方面舒普门限签名中签名的生成和验证是完全非交互的, 减少了不必要的传输开销; 另一方面舒普门限签名者身份防伪造, 实现了各个业务主体间的权利均分, 避免了滥用职权上传恶意业务记录. 下面给出这个协议中主要算法的详细步骤.

第一步: 需要由中台中设定的可信中心随机选取一个多项式 $f(x)$.

$$f(x) = \sum_{i=0}^{t-1} a_i x^i \bmod p, \quad (1)$$

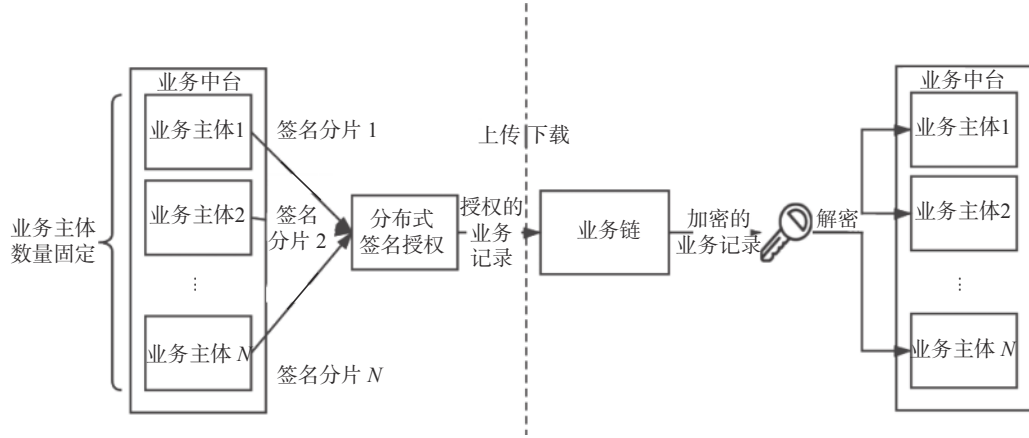


图 4 内生性数据交互协议——以业务中台和业务链为例

Fig. 4 Endogenous data interactive protocol—using the business platform and business chain as examples

其中 $a_0 = d$ 为初始密钥参数; p 为公共模数; t 为安全参数, 也称门限值.

第二步: 可信中心需要计算 d_j , $j \in \{1, \dots, N\}$, 作为对应业务主体的编号, 并将其发送给中台中相应的业务主体 B_j , 即:

$$d_j = f(j) \bmod p \rightarrow B_j. \quad (2)$$

同时, 可信中心还需要给出公钥对 (n, e) , 并计算 $L = l!$, l 为参与业务记录上链操作的业务主体总数.

第三步: 由各个业务主体 B_j 计算业务记录 m 的摘要哈希并进行签名分片:

$$\text{SigSlide}_j = H(m)^{2Ld_j} \bmod n. \quad (3)$$

第四步: 产生聚合签名, 首先根据公式计算:

$$\text{SigSlide}_j^2 = H(m)^{4Ld_j} \bmod n, \quad (4)$$

然后根据拉格朗日插值公式计算得:

$$y = H(m)^{4L^2d} \bmod n. \quad (5)$$

令 $e' = 4L^2$, 根据扩展欧几里得算法可以得知存在 a 和 b 使得 $ae + be' = 1$, 所以可以得出最后的聚合签名:

$$\text{sigM} = x^a y^b \bmod n. \quad (6)$$

第五步: 由链上合约验证聚合的门限签名是否正确, 按照如下公式进行判断:

$$\text{sigM}^e = H(m) \bmod n. \quad (7)$$

如果等式不成立, 则上链失败; 如果等式成立, 则表明签名有效, 允许将交易记录加密上链保存, 等到需要调用时, 再从链上拉取相关信息进行解密, 从而在一定程度上保障了内生性数据的交互安全.

3 实验验证及结果

本章将围绕数据上链前的数据交互, 先给出一个泛化场景的形式化证明和通用算法, 然后对此进行仿真模拟实验, 测试协议在数据交互上的效能.

3.1 形式化验证

为验证本研究中的链上链下数据协同技术是否合理有效, 率先给出形式化证明的算法流程图加以分析, 如图 5 所示.

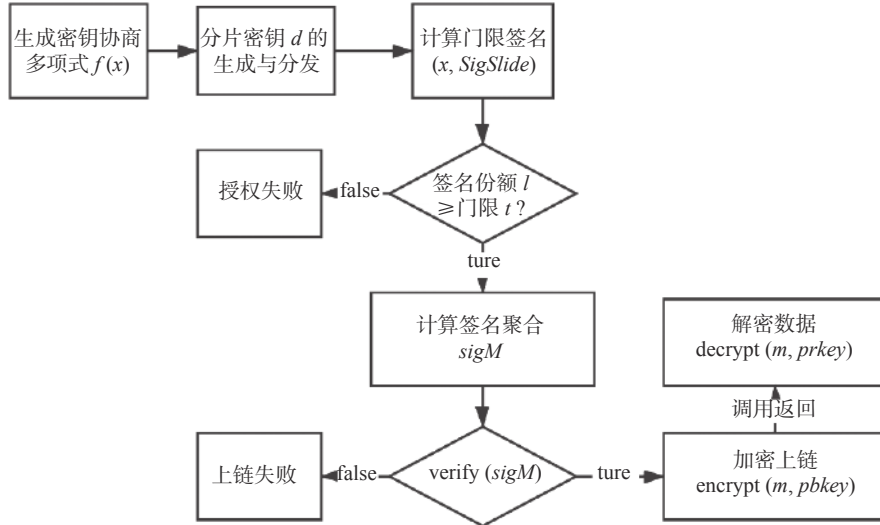


图 5 算法流程示意图

Fig. 5 Algorithm flow diagram

结合图 5 所示的算法流程图, 首先, 算法第一步是根据公式 (1) 生成密钥协商的多项式; 其次, 根据公式 (2) 构造出分片密钥 d , 通过匿名信道分发给业务主体或者数据主体.

在此基础上, 给出业务记录或者数据信息的门限签名, 并判断签名人数是否达到门限规定数量, 如果没有, 则授权失败, 无法进行下面的操作; 如果达到门限规定数量, 就根据公式 (4) — (6) 计算一个聚合的签名 sigM ; 接着就按照公式 (7) 交由合约验证, 判断签名的合法性. 如果不合法, 业务记录或数据信息就会上链失败; 如果合法, 即调用加密函数 $\text{encrypted}(\cdots)$ 进行业务记录或数据信息的加密上链操作, 加密方式如下.

$$C_{\text{encrypted}} = C_{\text{message}}^{k_{\text{pbkey}}}, \quad (8)$$

其中 C_{message} 是需要加密的消息, k_{pbkey} 是加密使用的公钥. 最后如果需要查询链上存储的内容, 那么就调用解密函数 $\text{decrypted}(\cdots)$, 解密方式如下.

$$C_{\text{decrypted}} = C_{\text{encrypted}}^{k_{\text{prkey}}}, \quad (9)$$

其中 k_{prkey} 是解密使用的私钥. 获得解密后的业务记录或数据信息的明文后, 一个完整的形式化证明流程才算结束.

从上述形式化证明中可以看出, 数据上链前经过了两轮质询, 一是数据传输时签名人数的核验; 二是聚合签名的核验, 保证了数据的安全传输. 而数据上链后是经过特定算法函数加密处理的, 调用时只需要用对应的解密函数进行解密, 就可以获得完整可信的数据明文信息.

3.2 通用算法设计

本节将从算法层面介绍链上链下数据协同的过程, 数据交互调用的伪代码如下.

Begin

Input:

callerId; //调用者 ID

```

    operation; //操作
    operationId; //操作标识符, 是业务操作还是数据操作
    sigM: [SigSlide_1, SigSlide_2, ..., SigSlide_N]; //sigM 为聚合签名, SigSlide 为单个调用者签名分片
Output:
    message; // 布尔类型, 表示上链操作是否成功
Load Input; //载入链下传入合约的信息流
If(!verifySig(callerId, sigM)) // 验证聚合签名消息是否合法
Return false;
If(operationId = 1) // 判断执行哪种操作
    executeBusiness(); //执行业务操作
Else if(operationId = 2)
    executeData(); //执行数据操作
Else
    Return false;
If(saveToContract(callerId, operation, sigM)) //保存相关信息到链上
    Return true;
Else
    Return false;
End

```

算法的第一步需要载入调用者的相关操作信息流;第二步需要验证聚合签名的有效性,判断聚合签名者的身份是否合法,以及聚合签名中签名人数是否达到指定标准,即判断有多少签名分片;第三步检查具体的操作内容,根据 operationId 分析具体的操作是业务操作还是数据操作,然后再分发到不同的链上合约进行处理;第四步是业务记录或数据信息的上链存储操作,通过智能合约添加新的内容到区块链上进行安全保存。

3.3 内生性数据交互过程的仿真模拟

为了进一步说明内生性数据交互协议的可行性,抽离出协议中对提升内生性数据交互效能起关键作用的门限签名算法进行模拟仿真实验,以业务中台和业务链之间的交互为例,设定门限为6,进行签名的业务主体签名人数为13的方案,进行相应的编码测试。在此次测试中,主要硬件环境如下:英特尔双核 i7 处理器 2.5 GHz、内存 8 GB、Win10 系统 64 位。

对于单次内生性数据交互,基于改进的协议签名编码测试结果如图6所示。

从图6中可以看出,消息 m 、聚合签名、模 n 后的聚合签名、消息摘要都是以大数形式展现的数字流。且根据前面的验签公式(7)不难看出,聚合签名 e 次幂模 n 后的签名数字流和消息摘要模 n 后的数字流内容一致,从而证实了图6中的验签过程合法有效。

虽然在图6中给出了加密消息 m 、聚合签名等签名、验签过程中的关键数据内容,但并未阐明这些数据与业务链之间的交互关系。图7给出在同样硬件环境中用开源智能合约开发环境 Remix 测试基于业务链的数据上传及下载的两个主要函数接口。

图7中,数据上传的主要函数接口为 addMessage(), 需要由指定业务主体将对应授权之后的聚合签名的字节码值以及经过加密函数 encrypted(...) 处理后的加密消息 m 的字节码值传入该函数接口,然后在函数接口内部判断签名无误后,再把加密消息 m 的字节码值上传到业务链上指定区块中进行存储。等到需要下载时再通过另外的函数接口 getMessage(), 输入需要查询的相应区块信息的映射编

号,接着就可以获取之前上链存储的指定聚合签名以及链上待解密的消息 m .最后再调用`decrypted(...)`函数对加密消息进行解密,即可获得相关的业务记录.此外,返回值中还可以获取先前指定业务主体的地址信息,方便业务中台内部跟踪数据源主体,以便进行有效监管.

```

可信中心: 测试512 bit 密钥...
可信中心: 正在尝试产生公钥对(n,e)...
私钥分片等可信参数产生时间共计 (ms): 1141
测试签名数总计 (6 个) 消耗时间(ms): 9
加密的消息m的大数值:
47766999897375391482600099239159488864404812178125115364455580128810335684946406
24707691790836980842295485374607006965906840297300494221623932809865442260777384
97387168603853943618153995642370692269183717993145840033782254680102955593562363
69658450568547554242786881647337378928814613124262499060990784141243
聚合签名的大数值:
24247299501888728534677408085888166429814874679884575752930172337687553660918685
12684616502936690475555059241884227643919449276114996137735375290961788979589615
25974008885566898775242359927770289104333615908822296268888987449837083280623460
80638282063256085228827297914804077051886418423950009874433769084227
聚合签名e次幂模n后的大数值:
34301711569450140466622303833219508809380084469814106405083971018262499519444237
68790764157633156031802682672503354882926767670283867554441744592834148967677070
48459678877487881601258326673724666959908631441117328612424945491519480531603450
58973043849460900846958385151729024848811454479017793460563688156328
消息摘要模n后的大数值:
34301711569450140466622303833219508809380084469814106405083971018262499519444237
68790764157633156031802682672503354882926767670283867554441744592834148967677070
48459678877487881601258326673724666959908631441117328612424945491519480531603450
58973043849460900846958385151729024848811454479017793460563688156328
测试签名数共计 (1 个) 消耗时间(ms): 75

```

图 6 单次签名验签测试结果图

Fig. 6 Unit testing about results of signature and verification

The screenshot displays a web application interface for managing business chain data. It features two main sections: 'addMessage' and 'getMessage'.

- addMessage Section:**
 - 聚合签名 (Aggregated Signature):** The value is `343017115694501404666223038332195088093800844698141064050`.
 - 加密消息 (Encrypted Message):** The value is `477669998973753914826000992391594888644048121781251153644`.
 - A 'transact' button is visible.
- getMessage Section:**
 - A search input field contains the number '5' and the text '查询链上相应块信息的映射编号' (Query the mapping number of the corresponding block information on the chain).
 - 业务主体地址 (Business Entity Address):** The value is `address: 0xA0212591F8f7176fa467ABe4F20864D33695797D`.
 - 指定的聚合签名 (Specified Aggregated Signature):** The value is `string: 34301711569450140466622303833219508809380084469814106405083971018262499519444237 68790764157633156031802682672503354882926767670283867554441744592834148967677070 48459678877487881601258326673724666959908631441117328612424945491519480531603450 58973043849460900846958385151729024848811454479017793460563688156328`.
 - 链上获取的待解密的消息 (Message retrieved from the chain for decryption):** The value is `string: 47766999897375391482600099239159488864404812178125115364455580128810335684946406 24707691790836980842295485374607006965906840297300494221623932809865442260777384 97387168603853943618153995642370692269183717993145840033782254668603853943618153995642370692269183717993145840033782254680102955593562363 69658450568547554242786881647337378928814613124262499060990784141243`.

图 7 基于业务链的数据上传及下载函数接口

Fig. 7 Data upload and download parameter result graph based on a business chain

为了证实协议应用的门限签名算法能够有效提升内生性数据交互的效能, 本文分别设置了三组签名验签对照组, 依次为链下签名及验签对照组、链上签名及验签对照组以及基于改进的协议签名、验签对照组. 通过设定 20 次单体测试, 对每组的签名、验证的开销进行了详细分析, 每次测试的时间开销如表 1 所示. 在此测试中, 主要硬件环境如下: 英特尔双核 i7 处理器 2.5 GHz、内存 8 GB、Win10 系统 64 位.

表 1 三组签名及验签测试对照组的时间开销

Tab. 1 The overhead time for a control group with three sets of signatures and verification tests

实验次数	签名前可信参数	中台对照组-链下签名及验签		区块链对照组-链上签名及验签		基于改进的协议签名	
	产生时间/ms	签名花费时间/ms	验证花费时间/ms	签名花费时间/ms	验证花费时间/ms	签名花费时间/ms	验证花费时间/ms
1	1141	9	64	17 592	23 562	14	18 024
2	1050	9	54	15 756	22 290	13	15 174
3	972	10	47	14 490	21 366	14	18 852
4	1156	10	57	15 096	20 808	13	18 078
5	1052	10	43	10 896	17 058	13	18 930
6	1181	10	52	11 112	17 118	10	18 612
7	1274	10	61	11 520	16 398	12	25 680
8	1060	9	65	15 216	21 336	10	16 938
9	971	9	53	12 318	17 058	12	18 600
10	1339	9	64	12 132	17 184	9	21 924
11	1000	9	54	12 858	18 738	10	16 206
12	1301	9	48	11 142	16 938	15	16 866
13	985	9	53	11 352	16 998	11	18 540
14	1234	10	59	13 374	18 918	10	15 810
15	1027	10	52	12 174	18 126	11	18 834
16	1009	9	58	14 340	19 824	9	18 750
17	1160	9	50	14 220	20 400	13	23 478
18	1298	9	43	11 688	17 412	14	16 572
19	1041	9	48	12 792	18 498	9	18 048
20	1108	11	50	12 540	18 720	11	17 160

从表 1 中可以看到, 在 20 次单体测试中, 链下签名及验签实验对照组的签名和验签时间总体来说时间开销最短. 但是因为如果内生性数据交互在链下签名、验签, 则并未涉及区块链结构, 那么在业务溯源、数据安全方面就没有很好的保障, 也不具备实际应用价值. 所以主要分析后面两个对照组的签名、验签方面时间开销的结果. 链上签名及验签对照组将中台间内生性数据的签名、验签的过程全部交由区块链进行处理, 虽然在业务溯源、数据安全方面有所保障, 但是由于签名和验签时间普遍较长, 因此相应地, 数据交互处理的效能便会有所偏低. 所以, 综合来看, 采用协议设计的签名方案, 在链下签名后交由链上进行验签处理, 就可在提升中台间数据交互效能的同时, 借助区块链双链结构实现中台业务溯源、数据调度精准的目标, 并且保障数据可信安全.

为了更直观地对比在使用区块链技术的前提下,协议中的门限签名方案与传统单一链上签名、验签方案的时间开销,分别计算 20 次单体测试中两种方案各自签名与验签总花费时间开销的平均值,给出如图 8 所示的柱形图.从图 8 中可看出链上签名及验签算法的签名和验签总时间开销平均为 32 067.9 ms,而基于改进的协议签名算法链上签名及链下验签算法的签名和验签总时间开销平均为 18 563.3 ms.相比之下,协议签名算法节省了近 42.1% 的时间成本.

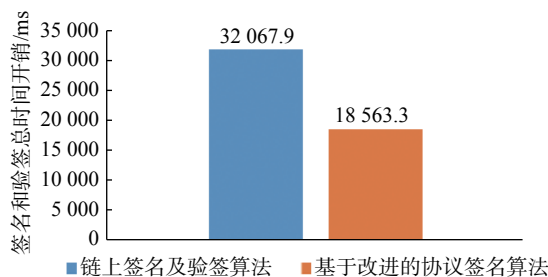


图 8 两种不同方案的签名及验签总时间开销对比柱形图

Fig. 8 Column chart comparing the total overhead time of signature and verification for two different schemes

综上,实验结果表明该协议算法在内生性数据交互过程中签名效率较高,验签效率相对较低,相对于传统单一链上签名、验签方式,协议在对内生性数据的交互处理上具有较高的效能.

4 讨 论

本研究从“数据+业务”的双中台架构设计出发,结合区块链双链技术,切入双中台数据上链到区块链中传输信道中内生性数据的交互效率问题,给出了一个高效交互的协议设计,主要的创新点如下.

(1) 通过将区块链技术导入中台,提升了内生性数据的交互安全,保证了中台数据上链前的可信性.构建了一种改进的舒普门限内生性数据交互协议来保障数据在上链前的安全性.

(2) 在上述工作的基础上设计了一个融合链下签名、链上验签的交互机制,提升了双中台双链的数据交互效率.实验结果表明,该机制降低了 42.1% 的时间开销,提升了中台与区块链两个体系间数据交互的效率.

当然,新协议仍然面临着以下挑战:首先,在技术层面上,还必须要融合其他技术,如大数据、人工智能等新技术,来持续优化中台技术结构.其次,在政策层面,要有国家对区块链技术的支持,鼓励实施优良技术标准和发布相关可信规范,在宏观调控上尽量避免技术作恶.最后,在业务层面上,需要继续细分业务结构,使得业务中台在提取数据中台相关信息时能更高效,从而增强业务处理能力.

5 结 论

本文提出了面向双中台双链架构的内生性数据交互协议,从算法公式推导上证实了协议的可实现性.针对中台与区块链两个体系间的数据协同给出了形式化验证,对协同的关键机制进行了实验模拟,结果表明该机制能够提升系统内生性数据间的交互效率.这种双中台双链体系架构下的新协议将会对“区块链+中台”的落地应用有一定的启示作用.当然,中台也仍然还是一个发展中的概念,中台在落地应用实践中还会不断产生新的问题与需求,这将是未来持续研究的方向.

[参 考 文 献]

- [1] 伊夫·莫里厄,李舒,阮芳,等.平台化组织:组织变革前沿的“前言”[J].哈佛商业评论,2016(10):108-134.

- [2] 谭虎, 陈晓勇. 详解阿里云数据中台, 一篇文章全面了解大数据“网红” [EB/OL]. 阿里数据. (2019-09-23) [2020-07-14]. <https://dp.alibaba.com/exchange/article?spm=a215hz.13439232.0.0.b2f54aa0InEHIF&artid=28>.
- [3] 邓立君. 数据中台与大数据中心分析 [J]. 电子世界, 2019(22): 85-86.
- [4] 宫志奇. 浅谈业务中台在港口的应用和挑战 [J]. 计算机产品与流通, 2019(10): 165.
- [5] 赵冠东, 张才俊, 欧阳红, 等. 基于业务中台的全渠道运营支撑平台架构设计研究 [J]. 供用电, 2019(6): 67-71.
- [6] 付威. 东方金信数据中台 [J]. 软件和集成电路, 2019(8): 98.
- [7] LI Z, YANG Y. RRect: A novel server-centric data center network with high power efficiency and availability [J]. IEEE Transactions on Cloud Computing, 2018: 914-927.
- [8] WIN N W, THEIN T. An efficient big data analytics platform for mobile devices [J]. International Journal of Computer Science and Information Security, 2015, 13(9): 1-10.
- [9] ANTHONY A, SHIH Y K, JIN R, et al. Leveraging a graph-powered, real-time recommendation engine to create rapid business value [C]// Proceedings of the 10th ACM Conference on Recommender Systems. 2016: 385-386.
- [10] 毕娅, 周贝, 冷凯君, 等. 基于双链架构的医药商业资源公有区块链 [J]. 计算机科学, 2018, 45(2): 40-47.
- [11] GAI K, CHOO K K R, ZHU L. Blockchain-enabled reengineering of cloud datacenters [J]. IEEE Cloud Computing, 2018, 5(6): 21-25.
- [12] LI H C, GAI K K, FANG Z K, et al. Blockchain-enabled Data Provenance in Cloud Datacenter Reengineering [C]// Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical (BSCI'19). New York: Association for Computing Machinery, 2020: 68-74.
- [13] SHOUP V. Practical threshold signatures [C]// International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2000: 207-220.

(责任编辑: 林 磊)