智能系统学报
CAAI TRANSACTIONS ON INTELLIGENT SYSTEMS

面向业务过程协同的隐私数据通信方法

陈建兵, 李子谦, 余阳, 潘茂林

引用本文:
陈建兵, 李子谦, 余阳, 等. 面向业务过程协同的隐私数据通信方法[J]. 智能系统学报, 2025, 20(2): 355-362.
CHEN Jianbing, LI Ziqian, YU Yang, et al. Private data communication method for business process collaboration[J]. *CAAI Transactions on Intelligent Systems*, 2025, 20(2): 355-362.

在线阅读 View online: https://dx.doi.org/10.11992/tis.202311018

您可能感兴趣的其他文章

差分隐私的高维数据发布研究综述
A research review of high-dimensional data publishing based on a differential privacy model
智能系统学报. 2021, 16(6): 989-998 https://dx.doi.org/10.11992/tis.202104023

基于多源异构数据融合的网络安全态势评估体系
Network security situation assessment architecture based on multi-source heterogeneous data fusion
智能系统学报. 2021, 16(1): 38-47 https://dx.doi.org/10.11992/tis.202006053

联邦推荐系统的协同过滤冷启动解决方法
Cold starts in collaborative filtering for federated recommender systems
智能系统学报. 2021, 16(1): 178-185 https://dx.doi.org/10.11992/tis.202009032

多智能体系统安全性问题及防御机制综述
A survey of the security issues and defense mechanisms of multi-agent systems
智能系统学报. 2020, 15(3): 425-434 https://dx.doi.org/10.11992/tis.201812015

基于区块链的公共数据电子证据系统及关联性分析
An electronic evidence system based on blockchain and correlation analysis
智能系统学报. 2019, 14(6): 1127-1137 https://dx.doi.org/10.11992/tis.201905058

基于MB-CSLBP的手指静脉加密算法研究
Finger-vein encryption algorithm based on MB-CSLBP
智能系统学报. 2018, 13(4): 543-549 https://dx.doi.org/10.11992/tis.201704034

DOI: 10.11992/tis.202311018
网络出版地址: https://link.cnki.net/urlid/23.1538.TP.20250107.1642.006

面向业务过程协同的隐私数据通信方法

陈建兵[1], 李子谦[1], 余阳[2], 潘茂林[2]
(1. 中山大学 计算机学院, 广东 广州 510006; 2. 中山大学 软件工程学院, 广东 珠海 510275)

摘　要: 将区块链应用于业务过程协同可以增强业务过程协同的可信性, 但是现有的数据通信方式存在影响数据可靠性和区块链可追溯性、泄露数据隐私等问题, 无法满足组织间正常业务过程协同的需求。为解决上述问题, 提出了一种面向业务过程协同的隐私数据通信方法, 拓展了 Wf-XML 2.0 协议, 并基于星际文件系统 (interplanetary file system, IPFS) 和非对称加密技术设计了代理组件 Broker, 将数据通信分为保存数据、请求数据和响应数据 3 个步骤执行来保障业务数据的隐私。通过 Dolev-Yao 攻击者模型、过程协同实际案例和实验对方法进行分析, 验证了该方法的安全性、合理性和可行性。

关键词: 区块链; 过程协同; Wf-XML 2.0; 非对称加密; 数据隐私; 互操作协议; 通信方法; Dolev-Yao
中图分类号: TP311.13　　**文献标志码**: A　　**文章编号**: 1673−4785(2025)02−0355−08

中文引用格式: 陈建兵, 李子谦, 余阳, 等. 面向业务过程协同的隐私数据通信方法 [J]. 智能系统学报, 2025, 20(2): 355–362.
英文引用格式: CHEN Jianbing, LI Ziqian, YU Yang, et al. Private data communication method for business process collaboration[J]. CAAI transactions on intelligent systems, 2025, 20(2): 355–362.

Private data communication method for business process collaboration

CHEN Jianbing[1], LI Ziqian[1], YU Yang[2], PAN Maolin[2]
(1. School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou 510006, China; 2. School of Software Engineering, Sun Yat-sen University, Zhuhai 510275, China)

Abstract: The application of blockchain to business process collaboration enhances its credibility. However, existing data communication methods encounter issues such as compromising data reliability, blockchain traceability, and data privacy. As a result, they fail to meet the needs of standard business process collaboration between organizations. We propose a private data communication method for business process collaboration to solve these problems. This method extends the Wf-XML2.0 protocol and designs a Broker component based on the interplanetary file system and asymmetric encryption technology. Data communication is divided into three steps to ensure the privacy of business data: saving, requesting, and responding. We use the Dolev–Yao attacker model, practical cases of process collaboration, and experiments for analysis to verify the security.

Keywords: blockchain; process collaboration; Wf-XML 2.0; asymmetric encryption; data privacy; interoperation protocol; communication method; Dolev-Yao

在现代商业环境下, 为了实现共同的商业目标, 每个企业的业务过程常常需要与其他企业的业务过程进行交互和协作, 形成协同优势并满足商业需求[1], 这种复杂过程被称为业务过程协同[2]。为了增加业务过程协同的信任度和透明度, 区块链技术[3]被引入, 用于记录业务过程协同中各个企业的互操作行为。在区块链环境下, 业务过程协同可以按照约定的顺序进行, 并且协同的互操作信息不可篡改且可追溯审计[4]。

在业务过程协同中, 现有的数据通信方式主要有 2 种: 1) 使用 Wf-XML 2.0 协议[5]规定的方式传递数据。Wf-XML 2.0 协议是一个工作流引擎之间的互操作标准, 在数据通信时使用统一资源标识符 (uniform resource identifier, URI) 进行数据

收稿日期: 2023−11−15.　**网络出版日期**: 2025−01−08.
基金项目: 国家重点研发计划项目 (2020YFB1707603); NSFC-广东联合基金项目 (U20A6003); 国家自然科学基金项目 (61972427); 广东省科技计划项目 (2020A0505100030).
通信作者: 余阳. E-mail: yuy@mail.sysu.edu.cn.

©《智能系统学报》编辑部版权所有

传递。然而，使用该方式进行数据通信时会将URI 记录于区块链上，此时业务数据的可靠性和区块链的可追溯性会受到影响。一方面通过URI 所能获取到的数据内容能被数据拥有者修改，另一方面区块链中的 URI 也会因实际数据的存放位置改变而失效，这两方面原因有可能导致业务过程协同的其他成员获取到错误的数据或者获取不到数据，从而影响数据的可靠性，也导致区块链没有数据的操作记录而影响可追溯性。2) 直接通过区块链传递数据。使用这种方式传递数据时，各个成员节点会复制该数据以保证区块链的不可篡改性，当数据过多或者过大时就会给区块链系统带来严重的存储开销。这 2 种数据传递方式都无法满足正常的业务过程协同需求。

此外，在业务过程协同中引入区块链会有泄漏数据隐私的风险。一般情况下，业务过程协同中对数据的要求为部分成员可见，而区块链上的记录对所有成员都是可见的，这导致了组织对数据隐私泄露的担忧[6-7]。由此可见，在基于区块链的业务过程协同中数据通信仍存在挑战。

为了保持数据的可靠性、区块链的可追溯性以及解决数据隐私泄露问题，本文提出了一种面向业务过程协同的隐私数据通信方法，其贡献在于：1) 拓展了 Wf-XML 2.0 协议，使业务过程管理系统 (business process management system, BPMS)[8] 能够对 Activity 的自定义字段进行操作从而支持基于区块链的业务过程协同的数据通信；2) 结合 IPFS(inter planetary file system)[9] 和非对称加密[10] 技术设计了面向业务过程协同的隐私数据传输方法及相应的算法；3) 分别通过 Dolev-Yao 攻击者模型[11]、实际案例、实验验证该方法的安全性、合理性、可行性。

1　相关工作

目前已有不少研究将区块链技术应用于电子数据[12-13]、电子健康记录[14]、金融市场[15]、能源供应[16]、供应链[17] 和物联网[18] 等领域，同样也有不少研究推动了区块链技术与业务过程管理领域的集成。Corradini 等[19] 提出了一种利用 BPMN 模型来描述过程协同的方法，并基于区块链实现 FlexChain 框架，解决了过程协同灵活性不够的问题。Fang 等[20] 提出了一个理论框架和方法，用于解决区块链网络在制定工作流服务之间互操作性的建模问题。Suliman 等[21] 基于区块链提出 BlockCheck 框架，为复杂 BPMN 流程模型提供可信的一致性检查。López-Pintado 等[22-23] 实现了 Caterpillar 流程引擎，从而实现了流程实例状态的监控和流程任务的执行功能，并且解决了任务实例没有操作权限的问题。

总体而言，将区块链技术集成到业务过程管理领域中的研究还处于比较早期的阶段[24]，而且多数研究是一种仅适用于单个组织或公司的集中式架构，难以直接应用于业务过程协同。另外，不同企业的 BPMS 通常是异构的，将区块链应用于业务过程协同时异构的 BPMS 需要进行适配，这也成为组织间业务过程协同的一个阻碍。为了能在区块链环境下支持组织间的业务过程协同并支持标准化，唐玄昭等[25] 此前提出一个基于区块链的业务过程协同框架。然而这个框架还不能解决在协同过程中的数据隐私问题。因此，需要有一个安全、合理、可行的隐私数据通信方法来解决基于区块链的业务过程协同中的数据隐私问题。

2　隐私数据通信方法设计

2.1　方法框架

本文提出的隐私数据通信方法基于图 1 的业务过程协同框架。框架的主要功能模块有 Broker、IPFS、控制模块和通信模块。

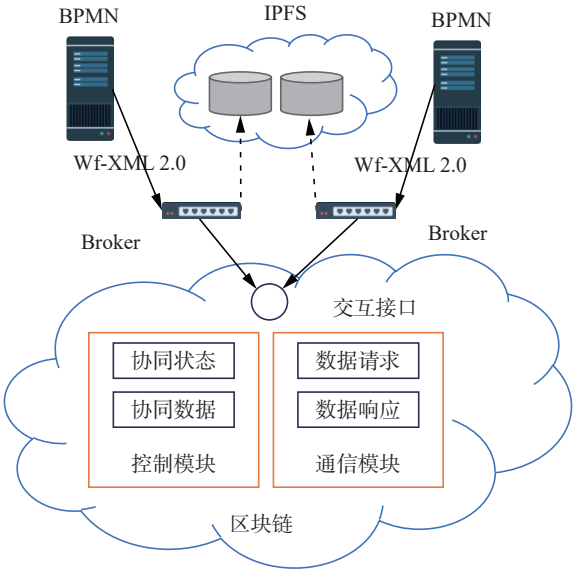


图 1　业务过程协同框架

Fig. 1　Business process collaboration framework

Broker　Broker 是工作流引擎和区块链中间的操作代理，将 Wf-XML2.0 协议映射为区块链的概念和操作，从而接收工作流引擎的的互操作请求，调用区块链功能，并保存了区块链的一些关键信息 (区块链成员身份信息、公钥对应关系及自身区块链私钥等)。

IPFS　IPFS 是一种新型的去中心化存储架构，提供了一种更加安全、方便集成的链下存储

解决方案。IPFS 存储时将业务数据划分成固定大小的块, 根据内容计算哈希值, 块组合后再计算完整的业务数据地址哈希。本文后续将这个地址哈希简称为地址, 只有通过该地址才能向 IPFS 获取到原始的业务数据。如图 2 所示, 本文将 Broker 和 IPFS 结合, 用以实现上传和获取业务数据的功能。

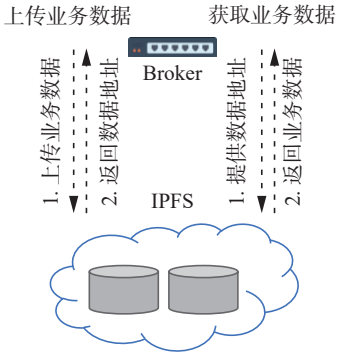


图 2　使用 IPFS 上传和获取数据

Fig. 2　Upload and retrieve data using IPFS

控制模块　控制模块是控制着业务过程协同正常进行的智能合约。控制模块代表业务过程协同实例, 协同状态代表 BPMS 的互操作行为, 加密地址记录着加密后的数据地址。可以同时存在多个过程协同模块, 表示多个业务过程协同在同时进行。

通信模块　通信模块是用于业务数据发送获取的智能合约。数据请求记录了数据请求者对控制模块中加密地址的请求信息, 数据响应记录了数据拥有者对请求的响应信息。在本文框架中仅用一个通信模块来进行数据通信。

2.2　Wf-XML2.0 协议拓展及映射

工作流管理联盟 (workflow management coalition, WfMC) 对业务过程协同有深入的研究, 在 WfMC 提出的工作流管理模型中, 定义了一个工作流引擎间的互操作接口[26]。随着网络技术的发展, Wf-XML 2.0 协议作为工作流引擎间的互操作标准被提出, 定义了工作流引擎间的互操作接口标准。由于在本文的框架中工作流引擎实际上是与区块链进行互操作, 所以需要将 Wf-XML 2.0 协议的概念映射为区块链的概念。Wf-XML 2.0 的基本概念映射如表 1 所示。

Wf-XML 2.0 协议规定的方式无法满足正常的业务过程协同需求, 为了保持引入区块链带来的可信性和支持 Broker 的自动化, 本文拓展了 Wf-XML 2.0 协议, 具体的概念映射如表 2 所示。在对 Wf-XML2.0 协议进行映射时, Activity 实际上对应 BPMS 在一个协同流程实例中的一次互操作行为。因此, 本文在拓展时将 ActivityData 定义为协同流程实例 Activity 中某个自定义字段, 将 SetActivityData 和 GetActivityData 分别定义为对 ActivityData 的设置和获取操作。本文将数据通信视为一个带有数据的互操作行为, 同时要求数据有访问控制列表用以保护数据隐私, 因此本文的 ActivityData 特指原始数据和访问控制列表。

表 1　Wf-XML2.0 与区块链的基本概念映射

Table 1　Mapping of basic concepts between Wf-XML 2.0 and blockchain

Wf-XML 2.0	区块链	说明
Factory	智能合约定义	流程模型
Activity	智能合约上的操作	流程实例中的等待点
CreateInstance	部署智能合约	创建流程实例
Complete-Activity	调用智能合约的操作	Activity完成
StateChanged	区块链的emit事件	流程实例状态更改

表 2　Wf-XML2.0 拓展内容与区块链的概念映射

Table 2　Mapping of extended concepts between Wf-XML 2.0 and blockchain

Wf-XML 2.0	区块链	说明
ActivityData	智能合约定义的字段	流程实例中Activity的自定义字段
SetActivityData	智能合约的操作	设置ActivityData的值
GetActivityData	智能合约的操作	获取ActivityData的值

2.3　方法步骤与算法设计

拓展了 Wf-XML2.0 协议后, Broker 也需要根据新的协议内容进行相应的设计与实现, 满足在区块链场景下业务过程协同的数据通信需求。同时为了使 BPMS 对数据传输的隐私保护无感知, 本文对 Broker 拓展了自动化的隐私数据通信功能。本文将 Broker 的隐私数据通信分为保存数据、请求数据和响应数据 3 个步骤, 并为每个步骤的执行设计了算法。SetActivityData 和 GetActivityData 执行时的工作流程分别如图 3 和图 4 的时序图所示。本文将保存数据的一方称为拥有方, 请求数据的一方称为请求方。

SetActivityData　如图 3 所示, 拥有方的 BPMS 通过调用 SetActivityData 接口发出保存数据的请求, Broker 将数据保存到 IPFS 中从而获得数据地址, 设置该数据的访问控制列表并加密数据地址, 在控制模块上保存加密地址。

GetActivityData　如图 4 所示, 请求方的 BPMS 通过 GetActivityData 接口发出获取数据的请求, 请求方的 Broker 收到请求后通过通信模块向拥有方请求原始数据, 拥有方的 Broker 同样通

过通信模块的智能合约发送响应数据的结果。请求方的 Broker 收到数据响应结果后进行验证，成功后向 IPFS 获取原始数据。

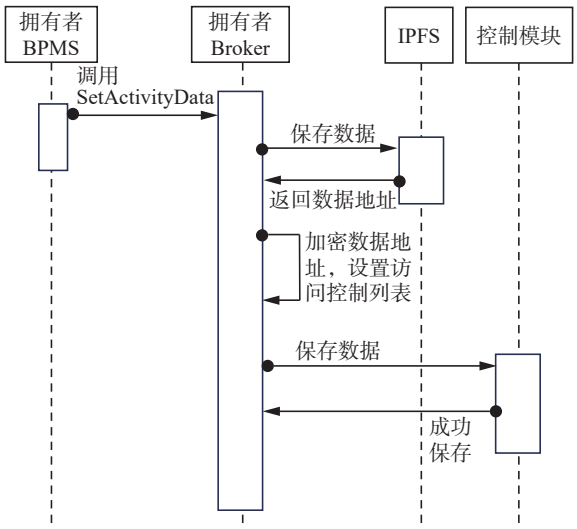


图 3　SetActivityData

Fig. 3　SetActivityData

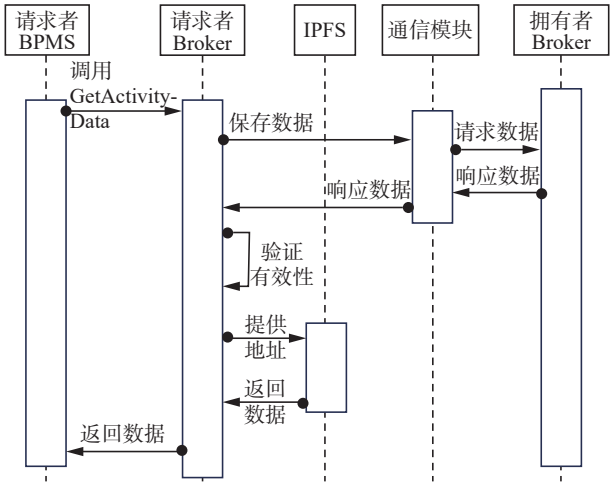


图 4　GetActivityData

Fig. 4　GetActivityData

在 GetActivityData 的时序图中拥有方的 BPMS 没有参与该过程，因为在 SetActivityData 时拥有方设置了数据的访问控制列表，此时拥有方的 Broker 根据数据的访问控制列表自动执行并返回结果。

本文方法在进行数据通信时需要使用图 1 中的控制模块和通信模块来支持算法的实现。保存数据、请求数据和响应数据 3 个数据通信步骤的算法如下。

保存数据　Broker 将数据 d 存储到 IPFS 上并获取业务数据的地址 a，使用拥有方的区块链公钥 p_{own}(后续区块链的公钥和私钥简称为公钥和私钥) 对数据地址 a 进行非对称加密，将加密后数据地址 e_a 存储到控制模块上，在 Broker 设置该数据的访问控制列表 l_a 供后续数据响应步骤的自动执行，该步骤如算法 1 所示。通过执行该算法，控制模块上记录的加密地址仅有拥有者能使用私钥解密出原始数据的地址。

算法 1　保存数据

输入　业务数据 d，访问控制列表 l_a，拥有方公钥 p_{own}。

1) 通过 IPFS 保存 d，获得地址 a

2) 使用 p_{own} 加密 a，获得 e_a

3) 调用智能合约将 e_a 保存到控制模块

4) 将 e_a 的访问控制列表设置为 l_a

请求数据　Broker 通过通信模块发起数据请求，数据请求的内容为控制模块中的加密地址 e_a，随后等待数据拥有方的数据响应结果 r。成功获取数据时，数据响应结果 r_a 为数据请求者公钥 p_{req} 对数据地址 a 的加密结果。此时，请求者的 Broker 通过自身私钥 s_{req} 还原出数据地址 a'，并用数据拥有者公钥 p_{own} 再次对 a'加密获得 e_a'，验证 e_a'是否与 e_a 一致，从而判断数据是否与过程协同模块上的记录一致。该步骤如算法 2 所示。通过执行该算法，通信模块上记录的数据请求，仅拥有者能使用私钥解密出原始数据的地址。

算法 2　请求数据

输入　数据加密地址 e_a，请求方私钥 s_{req}，拥有方公钥 p_{own}。

输出　ret(原始数据或者 NULL)。

1) 使用 e_a 通过数据模块请求数据，获得响应 r_a

2) IF $r_a \neq$ NULL THEN

3) 使用 s_{req} 从 r_a 还原出数据地址 a'

4) 使用 p_{own} 再次加密 a'得到 e_a'

5) IF $e_a' == e_a$ THEN

6) 使用 a'从 IPFS 获取数据 d

7) ret = d

8) END IF

9) END IF

10) RETURN ret

响应数据　Broker 收到数据请求自动执行返回结果。Broker 使用自身私钥 s_{own} 还原数据请求内容 e_a 得到数据地址 a，判断请求者是否在访问控制列表 l_a 里，返回一个空数据响应，或请求者的公钥 p_{req} 对 a 的加密结果 r_a。该步骤如算法 3 所示。通过执行该算法，数据通信模块上记录了该数据响应，仅有请求者能使用私钥还原出原始地址。

算法 3　响应数据

输入　数据加密地址 e_a，请求方私钥 s_{own}，拥有方公钥 p_{req}。

输出　ret(加密地址或者 NULL)。

1) 初始化 ret 为 NULL

2) 使用 s_{own} 从 e 还原出数据地址 a

3) IF p_{req} 在 a 的访问控制列表 l_a 里 THEN

4) 使用 p_{req} 加密 a 获得加密地址 r_a

5) ret = r_a

6) END IF

7) RETURN ret

3　方法验证

3.1　安全性

本文使用 Dolev-Yao 攻击者模型对本文所提方法的安全性进行分析。Dolev-Yao 攻击者模型在既定完善的密码系统的基础上分析安全协议的正确性、安全性和冗余性等, 该模型刻画了攻击者的行为: 窃听和拦截所有经过网络的消息、存储拦截到的或自己构造的消息、发送拦截到的或自己构造的消息以及作为合法主体参与协议的运行。由于区块链的数据共享, 区块链网络中所有成员都是潜在的攻击者。下面将通过 Dolev-Yao 攻击者模型的形式化描述[27] 分析攻击者于本文方法框架中是否能窃取到业务数据。

定义以下符号:

S_{PKS}, 区块链所有成员公钥的集合。

P_X, 成员 X 的公钥。

S_X, 成员 X 的私钥。

$P_X(I)$, 使用 P_x 加密信息 I。

$S_X(I)$, 使用 S_x 解密信息 I。

假设有 3 个成员: 攻击者 A, 拥有者 O, 请求者 R。O 直接将数据或者数据的 IPFS 地址 a 保存在区块链中是不安全的, 因为 A 可以轻松获取。而使用本文通信方法时, O 在执行保存数据步骤后, A 的信息集 T 为

$$T = \{S_{PKS}, S_I, P_O(a)\}$$

R 执行请求数据且 O 执行相应数据后, A 的信息集 T 更新为

$$T = \{S_{PKS}, S_I, P_O(a), P_R(a)\}$$

由于本文方法使用了非对称加密, 因此有以下关系:

$$a = S_O(P_O(a)) = S_R(P_R(a))$$

因此, 通过本文方法传输数据后, A 只能通过 S_O 或 S_R 来获取数据地址 a, 由于 S_O 和 S_R 都不在攻击者 A 的信息集 T 里, A 无法获取到原始的数据, 从而说明本文方法的安全性。

3.2　合理性

本小节通过一个实际案例分析本文方法的合理性。图 5 是一个论文审查协同流程模型[28], 该过程协同有 1 个程序委员会主席、3 个审核专家和 1 个联系作者, 假设这些成员分别代表不同组织的 BPMS, 本文仅关注程序委员会主席向 3 个审核专家发送评审请求这一数据通信部分。不妨假设数据包含了业务数据 (比如评审请求里包含了论文), 按照 Wf-XML 2.0 协议的方式和或直接通过区块链传输的方式进行数据传输时会将业务数据的信息保存在区块链上。由于区块链上的数据对所有成员可见, 当区块链中存在其他的联系作者时, 业务数据可以轻易被其他联系作者获取, 这极其不合理。

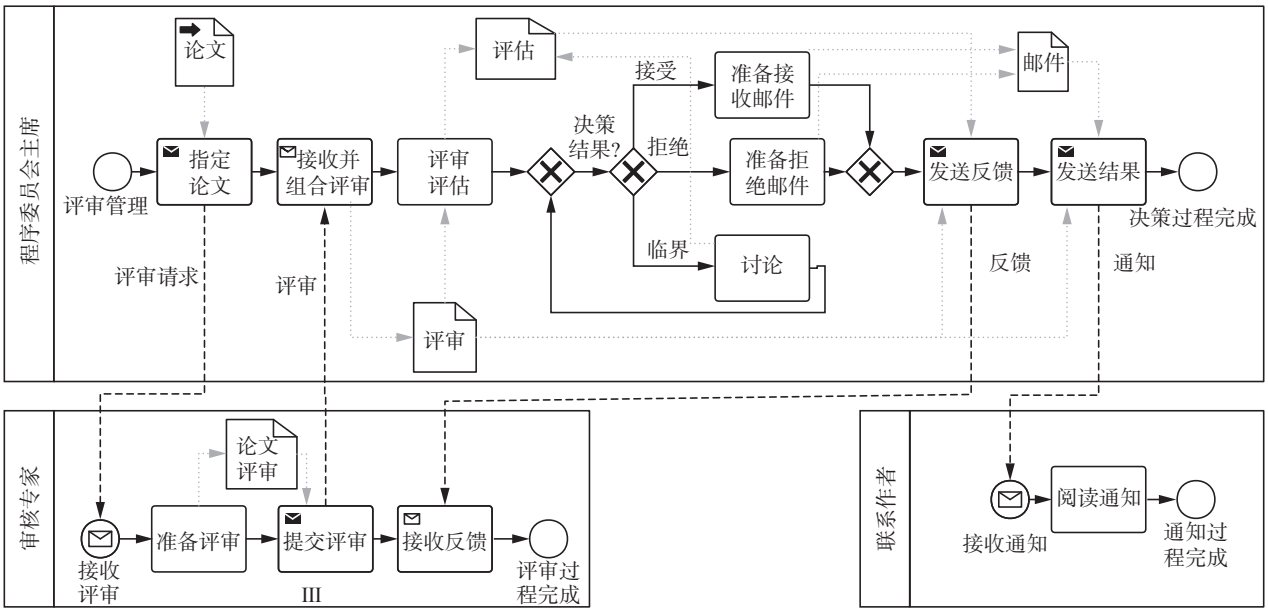


图 5　论文审查协同流程模型

Fig. 5　Collaborative process model for paper review

显然，对数据进行加密传输是非常必要的。然而在本文的方法框架上 (如图 1 所示)，还存在着一对一的非对称加密数据通信方法 (简称一对一方法)。就图 5 的论文审查协同流程而言，程序委员会主席向 3 个审核专家发送评审请求这一数据通信部分使用一对一方法需要分别对每一个审核专家发送加密数据地址，对应着图 1 控制模块中的 3 个协同状态和 3 个加密地址字段。而 1 个协同状态代表着 BPMS 的 1 次互操作行为，所以程序委员会主席在发送同样的评审请求时，需要执行 3 次互操作行为。在审核专家数量不同的情况下，程序委员会主席需要执行的互操作行为次数等同于审核专家的个数，当有大量的审核专家时，论文审查协同的互操作行为次数就非常不合理。

相比之下，本文的方法不仅使用了非对称加密技术，而且通过访问控制列表实现 Broker 的自动化执行，所以程序委员会主席发送评审请求需要 1 个协同状态记录程序委员会主席的保存行为，1 个加密地址用来记录程序委员会主席传输的加密地址。图 6 为一对一非对称加密通信方法 (记为一对一方法) 和本文方法的协同开销对比 (协同状态个数或加密地址个数)，不难发现一对一方法的协同开销会随着数据接收对象数量增加而线性增加，而本文方法的协同开销固定为 1 个协同状态和 1 个加密地址。由于在不同数据接收对象的情况下一对一方法需要进行多次互操作行为，而本文方法仅需进行一次互操作行为，所以本文方法更加合理。

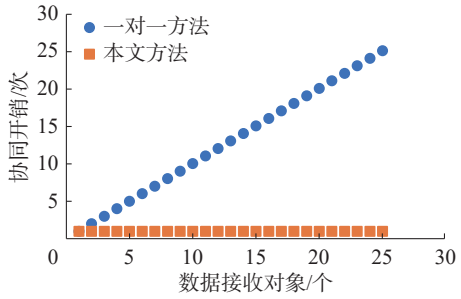


图 6　协同开销
Fig. 6　Collaboration cost

3.3　可行性

本小节将通过实验分析以下 3 种数据通信方法的开销: 1) 直接通信。通过区块链直接传输数据，记为方法 1。2) 使用非对称加密一对一通信。发送方使用非对称加密传输数据，接收方获取数据，记为方法 2。3) 使用本文方法通信，通过保存数据、请求数据和相应数据 3 个步骤传输数据，记为方法 3。实验内容为在使用不同大小的数据进行多次双方通信，对比上述 3 种方法的平均存储开销和运行时间开销，来验证本文方法的可行性。实验环境如表 3 所示。

表 3　实验环境
Table 3　Experimental environment

配置名称	配置信息
操作系统	Ubuntu 20.04
CPU型号	Intel(R) Xeon(R) Gold 5218R
区块链环境	长安链[29]
节点数量	4
非对称加密算法	国密SM4[30]

在区块链上传输数据时，除了存储该数据，还需要存储其他信息 (记为 C_m，视为常量)，故操作一次大小为 d 的数据的需要的存储空间 $M(d)$ 为

$$M(d) = (d+C_m)\times N$$

式中 N 为节点个数，假设节点同步速率为 S(视为常量)，操作一次大小为 d 的数据所需时间 $T(d)$ 为

$$T(d) = N\times(d+C_m)/S$$

对于数据操作次数，方法 1 和方法 2 需要 2 次 (保存 1 次，获取 1 次)，方法 3 操作 3 次数据 (对应本文方法 3 个步骤)。对于数据的大小，方法 1 为原始数据大小 d，方法 2 和方法 3 为数据地址大小 A(常量)。因此 3 种方法的时间和空间开销会有所不同。其中方法 1 的时间开销为 $2T(d)$，空间开销为 $2M(d)$，方法 2 的时间开销为 $2T(A)$，空间开销为 $2M(A)$，方法 3 的时间开销为 $3T(A)$，空间开销为 $3M(A)$。

在给定实验环境 $T(d)$ 以及 $M(d)$ 都为数据大小 d 的线性函数，故对实验结果有以下预测：方法 1 的时间与空间开销将与数据大小呈线性关系，方法 2 和方法 3 的时间与空间开销为常量，方法 3 相较于方法 2 开销多了 50%。通过表 3 的实验环境进行实验，3 种方法的运行时间开销和存储开销分别如图 7 和图 8 所示，基本与上述预测结果一致。

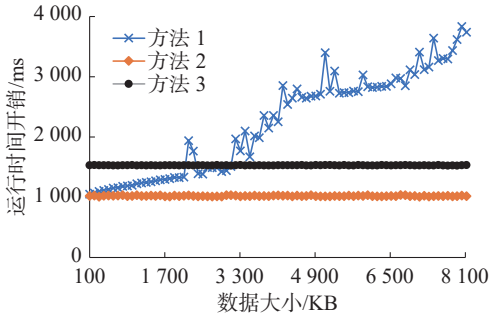


图 7　运行时间开销
Fig. 7　Runtime cost

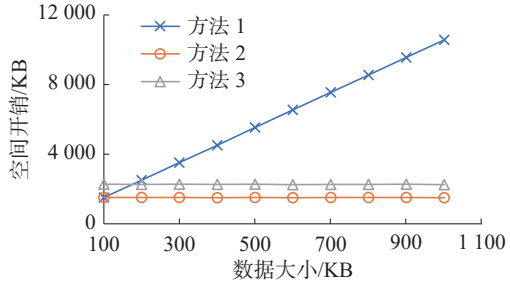


图 8　空间开销

Fig. 8　Memory cost

这个实验结果是基于双方的数据通信，但在过程协同中，普遍有多个数据接收方。假设有 n 个数据接收方，方法 2 需要操作 $2n$ 次数据 (保存数据 n 次，获取数据 n 次)，方法 3 需要操作 $1+2n$ 次数据 (保存数据 1 次，请求数据 n 次，响应数据 n 次)。如图 9 所示，本文方法开销相较于方法 2 增加的比例随接收方个数增加而降低，即成反比例关系。

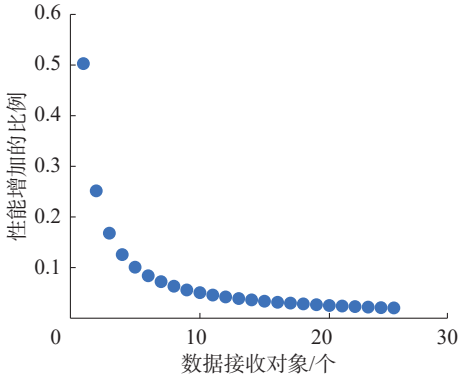


图 9　本文方法在时间、空间开销相较于方法 2 增加的比例

Fig. 9　Proportion of time and space cost increase in this method compared to method 2

本文方法在时间与空间二者的开销方面相比于方法 2 开销的增加比例在 3 个数据接收方时约为 16.7%，在 4 个接收方时约为 12.5%。在真实协同场景中，本文方法的时间开销通常会比方法 2 更小，这是因为方法 2 随着接收方个数的增加需要多次使用 BPMS 进行互操作行为，而这会增加更多的时间开销。因此，使用本文方法进行数据通信时的开销是可以接受的，本文方法具有可行性。

4　结束语

本文旨在为基于区块链的业务过程协同提供一个可信的数据通信方法。为实现该目标，本文提出了面向业务过程协同的隐私数据通信方法，该方法拓展了 Wf-XML2.0 协议进行数据通信，基于 IPFS 和非对称加密技术，将数据通信的过程设计成保存数据、请求数据和响应数据 3 个步骤，并为每个步骤设计相应的算法，从而使本文方法能够保障数据隐私。最后本文还对提出的数据通信方法进行验证：首先通过 Dolev-Yao 攻击者模型得出攻击者无法获取到业务数据的结论，从而验证安全性；其次通过过程协同实际案例分析得出本文方法相较于其他方法更加具有合理性；最后通过实验得出本文方法的运行时间开销和空间开销在可以接受的范围，从而验证方法可行性。

未来，希望基于区块链的业务过程协同框架能够应用于更加广泛的场景，但通常情况下，随着成员节点的增加区块链的性能会有所降低。因此，后续将考虑改进区块链共识机制来提高区块链性能，为基于区块链的业务过程协同带来效率上的提升。

参考文献：

[1] SUDUSINGHE J I, SEURING S. Supply chain collaboration and sustainability performance in circular economy: a systematic literature review[J]. International journal of production economics, 2022, 245: 108402.

[2] BAZAN P, ESTEVEZ E. Industry 4.0 and business process management: state of the art and new challenges[J]. Business process management journal, 2022, 28(1): 62−80.

[3] GUO Huaqun, YU Xingjie. A survey on blockchain technology and its security[J]. Blockchain: research and applications, 2022, 3(2): 100067.

[4] EDRUD P. Improving BPM with blockchain technology: benefits, costs, criteria & barriers[R]. Sundsvall: Mid Sweden University, 2021.

[5] SWENSON K D. ASAP/Wf-XML 2.0 Cookbook[EB/OL]. (2004−05−13)[2023−11−15]. https://groups.oasis-open.org/higherlogic/ws/public/download/4902/ASAP-Wf-XML%20Cookbook.pdf/latest.

[6] ZHANG Wenhua, QAMAR F, ABDALI T A N, et al. Blockchain technology: security issues, healthcare applications, challenges and future trends[J]. Electronics, 2023, 12(3): 546.

[7] HASAN M K, ALKHALIFAH A, ISLAM S, et al. Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations[J]. Wireless communications and mobile computing, 2022: 9065768.

[8] SZELĄGOWSKI M, LUPEIKIENE A, BERNIAK-WOŹNY J. Drivers and evolution paths of BPMS: state-of-the-art and future research directions[J]. Informatica, 2022, 33(2): 399−420.

[9] BENET J. IPFS-content addressed, versioned, P2P file system[EB/OL]. (2014−07−14)[2023−11−15]. https://arxiv.org/abs/1407.3561.

[10] BAMOTRA A. Cryptography and its techniques: a review[J]. Journal Punjab academy of sciences, 2022, 22(1): 28−33.

[11] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE transactions on information theory, 1983,

29(2): 198−208.

[12] 王琪, 张嘉政, 刘文奇. 一种基于区块链技术的公安执法电子证据系统的设计与实现[J]. 智能系统学报, 2022, 17(6): 1182−1193.
WANG Qi, ZHANG Jiazheng, LIU Wenqi. Design and implementation of a public security law enforcement electronic evidence system based on blockchain technology [J]. CAAI transactions on intelligent systems, 2022, 17(6): 1182−1193.

[13] 李萌, 刘文奇, 米允龙. 基于区块链的公共数据电子证据系统及关联性分析[J]. 智能系统学报, 2019, 14(6): 1127−1137.
LI Meng, LIU Wenqi, MI Yunlong. An electronic evidence system based on blockchain and correlation analysis[J]. CAAI transactions on intelligent systems, 2019, 14(6): 1127−1137.

[14] QU Zhiguo, ZHANG Zhexi, ZHENG Min. A quantum blockchain-enabled framework for secure private electronic medical records in Internet of Medical Things[J]. Information sciences, 2022, 612: 942−958.

[15] PATEL R, MIGLIAVACCA M, ORIANI M E. Blockchain in banking and finance: a bibliometric review[J]. Research in international business and finance, 2022, 62: 101718.

[16] GAWUSU S, ZHANG Xiaobing, AHMED A, et al. Renewable energy sources from the perspective of blockchain integration: From theory to application[J]. Sustainable energy technologies and assessments, 2022, 52: 102108.

[17] RAJA SANTHI A, MUTHUSWAMY P. Influence of blockchain technology in manufacturing supply chain and logistics[J]. Logistics, 2022, 6(1): 15.

[18] ABDELMABOUD A, AHMED A I A, ABAKER M, et al. Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions[J]. Electronics, 2022, 11(4): 630.

[19] CORRADINI F, MARCELLETTI A, MORICHETTA A, et al. Flexible execution of multi-party business processes on blockchain[C]//2022 IEEE/ACM 5th International Workshop on Emerging Trends in Software Engineering for Blockchain. Pittsburgh: IEEE, 2022: 25−32.

[20] FANG Yuchen, TANG Xuanzhao, PAN Maolin, et al. A workflow interoperability approach based on blockchain [C]//International Conference on Internet of Vehicles. Kaohsiung: Springer, 2020: 303−317.

[21] SULIMAN A T, KADADHA M, MIZOUNI R, et al. Blockcheck: a consortium blockchain-based conformance checking framework for business processes[J]. Internet of things, 2023, 21: 100652.

[22] LÓPEZ-PINTADO O, GARCÍA-BAÑUELOS L, DUMAS M, et al. Caterpillar: a business process execution engine on the Ethereum blockchain[J]. Software: practice and experience, 2019, 49(7): 1162−1193.

[23] LÓPEZ-PINTADO O, DUMAS M, GARCÍA-BAÑUELOS L, et al. Controlled flexibility in blockchain-based collaborative business processes[J]. Information systems, 2022, 104: 101622.

[24] GARCIA-GARCIA J A, SÁNCHEZ-GÓMEZ N, LIZCANO D, et al. Using blockchain to improve collaborative business process management: systematic literature review[J]. IEEE access, 2020, 8: 142312−142336.

[25] 唐玄昭, 余阳, 吴荆璞, 等. 基于区块链的业务流程互操作服务框架[J]. 计算机集成制造系统, 2021, 27(9): 2508−2516.
TANG Xuanzhao, YU Yang, WU Jingpu, et al. Business process interoperability service framework based on blockchain[J]. Computer integrated manufacturing systems, 2021, 27(9): 2508−2516.

[26] VIRIYASITAVAT W, BI Zhuming, HOONSOPON D. Blockchain technologies for interoperation of business processes in smart supply chains[J]. Journal of industrial information integration, 2022, 26: 100326.

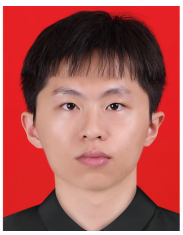
[27] 唐郑熠, 李祥. Dolev-Yao 攻击者模型的形式化描述[J]. 计算机工程与科学, 2010, 32(8): 36−38,45.
TANG Zhengyi, LI Xiang. The formalization description of the Dolev-Yao intruder model[J]. Computer engineering & science, 2010, 32(8): 36−38,45.

[28] CORRADINI F, MUZI C, RE B, et al. Animating multiple instances in BPMN collaborations: from formal semantics to tool support[C]//Interna-tional Conference on Business Process Management. Sydney: Spring, 2018: 83−101.

[29] YI Junkai, WANG Jin, TAN Lingling, et al. HMM-based blockchain visual automatic deployment system[J]. Applied sciences, 2024, 14(13): 5722.

[30] NIŞANCı G, FLIKKEMA P G, YALÇıN T. Symmetric cryptography on RISC-V: performance evaluation of standardized algorithms[J]. Cryptography, 2022, 6(3): 41.

作者简介：



陈建兵，硕士研究生，主要研究方向为业务过程协同、区块链技术。E-mail：chenjb58@mail2.sysu.edu.cn。

李子谦，硕士研究生，主要研究方向为业务过程协同、区块链存储优化。E-mail：lizq36@mail2.sysu.edu.cn。

余阳，教授，博士生导师，博士，主要研究方向为工作流技术、网络社会协同、服务计算技术、软件工程。主持完成国家级项目 8 项、省市级及其他项目 30 余项。获发明专利授权及软件著作权 30 项。发表学术论文 100 余篇。E-mail：yuy@mail.sysu.edu.cn。