计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2024,33(10):97−105 [doi: 10.15888/j.cnki.csa.009648]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于区块链的跨境贸易数据共享与访问控制方案①

李云鹏[1,2], 姜　茸[1], 梁志宏[3]

[1](云南财经大学 云南省服务计算重点实验室, 昆明 650221)
[2](云南财经大学 物流与管理工程学院, 昆明 650221)
[3](西南林业大学 大数据与智能工程学院, 昆明 650224)
通信作者: 姜　茸, E-mail: jiang_rong@aliyun.com

摘　要: 随着全球经济一体化的发展, 跨境贸易已成为全球经济发展的重要推动力量. 然而, 跨境贸易目前正面临着诸如数据安全、信息孤岛和信息不对称等问题. 基于此, 本文提出了一种基于区块链的跨境贸易数据共享与访问控制方案. 该方案采用区块链和星际文件系统 (IPFS) 结合的协同存储机制, 有效降低了区块链的存储负载. 另外, 利用了双密钥回归模型结合时间维度对数据进行加密和存储管理, 通过设定不同的时间段来进一步划分访问权限, 限制了数据用户对时间跨度范围外的非必要访问. 最后, 设计了相应的智能合约, 实现对数据整个周期流程的高效管控, 从而有效提升了数据共享操作的执行效率. 实验结果表明, 本方案能够实现跨境贸易数据的安全共享和对用户进行细粒度访问控制.

关键词: 跨境贸易数据; 区块链; 访问控制; 智能合约; 星际文件系统 (IPFS)

引用格式: 李云鹏,姜茸,梁志宏.基于区块链的跨境贸易数据共享与访问控制方案.计算机系统应用,2024,33(10):97–105. http://www.c-s-a.org.cn/1003-3254/9648.html

Scheme of Cross-border Trade Data Sharing and Access Control Based on Blockchain

LI Yun-Peng[1,2], JIANG Rong[1], LIANG Zhi-Hong[3]

[1](Yunnan Key Laboratory of Service Computing, Yunnan University of Finance and Economics, Kunming 650221, China)
[2](School of Logistics and Management Engineering, Yunnan University of Finance and Economics, Kunming 650221, China)
[3](College of Big Data and Intelligent Engineering, Southwest Forestry University, Kunming 650224, China)

Abstract: With the development of global economic integration, cross-border trade has become an important driving force for global economic development. However, it is facing issues such as data security, information silos, and information asymmetry. Based on this, this study proposes a blockchain-based scheme for data sharing and access control in cross-border trade. The scheme uses a collaborative storage mechanism of blockchain and inter planetary file system (IPFS) to effectively reduce the storage load of blockchain. In addition, a dual key regression model combined with time dimension is adopted to encrypt and store data, as well as assign access permissions by setting different time periods, which limits the unnecessary access of data users outside a certain time span. Finally, corresponding smart contracts are designed to achieve efficient management of the entire life cycle flow of data, improving sharing efficiency. The experimental results show that the proposed scheme can achieve secure data sharing in cross-border trade and fine-grained access control for users.

Key words: cross-border trade data; blockchain; access control; smart contract; inter planetary file system (IPFS)

① 基金项目: 云南省科技计划中央引导地方科技发展专项 (202307AB110009)
收稿时间: 2024-03-12; 修改时间: 2024-04-16, 2024-05-06; 采用时间: 2024-05-14; csa 在线出版时间: 2024-08-28
CNKI 网络首发时间: 2024-08-30

1 引言

2022 年我国货物贸易进出口总值 42.07 万亿元人民币, 比 2021 年增长 7.7%[1]. 跨境贸易规模的不断扩大, 伴随而来的是跨境贸易数据的海量增长. 但是由于跨境贸易数据的敏感性、隐私性、重要性, 各个贸易参与主体单独管理自身的贸易数据, 难以实现对内对外数据共享. 2020 年 10 月, 《国务院办公厅关于推进对外贸易创新发展的实施意见》指出, 要实现跨境贸易物流、商流、资金流、信息流等互联互通[2]. 2022 年 11 月, 商务部印发了《“十四五”对外贸易高质量发展规划》, 指出要坚持数字赋能, 加快数字化转型, 促进人工智能、大数据、区块链、云计算等相关技术与商贸企业深度融合应用, 打造贸易数字化交易平台[3]. 由此可见, 跨境贸易数据的存储和共享关乎规划的进行与目标的实现, 是打破贸易数据“信息孤岛”至关重要的一步.

虽然全球范围内跨境贸易的数字化转型正逐步得到普遍认可和推进, 但在实际操作层面, 特别是在涉及原产地证明、报关单据、信用证、检疫证明等多种关键贸易单证的流通环节, 各个参与方如海关、银行、保险公司等仍大量依赖传统的纸质文件来进行验证和确认. 这一现状带来的问题是显而易见的: 纸质单证的制作、邮寄、核验等环节造成的直接成本往往占据贸易总成本的 5%–10%, 同时还伴随着高昂的时间成本, 文件在传输过程中的延误以及人工审核的繁琐, 都会拖慢整个贸易流程[4]. 此外, 纸质单证较容易出现伪造、篡改等诚信风险. 要解决这些问题, 跨境贸易的核心挑战之一是构建一套既安全可靠又能实现高效共享和权限控制的数据交换体系[5]. 在多方参与的复杂跨境贸易环境中, 实现跨境贸易数据的共享与交换所面临的困境主要包括以下几个方面.

(1) 跨境贸易数据量大. 跨境贸易涉及大量数据, 包括商品信息、贸易单证、通关信息、物流信息、支付信息等, 每笔交易都会生成大量的数据记录.

(2) 信息不对称、数据孤岛问题. 各参与主体拥有独立的信息系统, 之间缺乏有效的数据交换和共享机制, 导致贸易相关的数据无法实现无障碍流通和实时更新.

(3) 贸易数据隐私保护问题. 跨境贸易数据往往涉及大量的个人信息和商业机密, 在数据共享过程中, 需要防止未经授权的访问和过度授权访问.

近几年来, 区块链技术兴起和蓬勃发展, 因其去中心化、不可篡改、可追溯等特点[6], 其与跨境贸易结合旨在解决传统跨境贸易中长期存在的痛点. 基于此, 本文提出一种基于区块链的跨境贸易数据共享与访问控制方案, 主要创新点如下.

(1) 针对跨境贸易数据量大、记录庞杂问题, 提出了链上和链下相结合方式对数据进行存储, 链上仅存储数据 Hash 值和存储位置, 链下通过星际文件系统存储完整数据, 减轻了区块链的负担.

(2) 针对贸易数据隐私保护问题, 采用双密钥回归模型, 由数据拥有者定义时间跨度, 根据贸易周期对跨境贸易数据进行加密、存储及共享, 对非必要数据进行保护, 杜绝用户过度访问.

(3) 针对共享效率低、流程繁琐问题, 设计了相应的智能合约实现对数据生命周期流转的管理, 提高了共享效率.

2 相关工作

2.1 区块链在跨境贸易领域应用现状

在跨境贸易领域, 区块链技术的应用正在引领一场深刻的变革. 新加坡的一家专注于金融科技解决方案的企业 (GeTS) 在 2018 年推出了一个名为 Open Trade Blockchain 的跨境贸易区块链平台, 其核心目标在于革新并优化贸易单证跨国验证的流程[7]. CargoX 公司在以太坊架构的基础上开发了一种开放源代码的区块链文档传输协议 (BDTS), 旨在为贸易单证及其他贸易过程中关键文件提供安全加密的存储及共享的解决方案[8]. Wave 等公司已成功利用概念验证模式对信用证支付流程进行了创新优化, 实现了首个基于区块链技术的实时贸易融资交易案例, 将原本可能需要数日才能完成的信用证交易周期缩短至 4 h 以内[9]. 随后, Wave 公司实施了海运行业首例试点项目, 并已推进至更广泛的验证阶段, 涵盖了 67 家银行、5 家运输公司及众多其他企业.

整体而言, 区块链技术在数字化贸易的进出口业务流程、海关通关环节、物流运输程序等方面已引起众多大型企业和政府部门的关注与兴趣. 然而, 在跨境贸易的具体场景下, 尽管潜力巨大, 但实际上全球范围内大规模应用和区块链项目的实例仍较为有限, 多数项目仍处在理论验证、初步实验和小范围试行阶段. 究其根本, 对于非金融行业应用如跨境贸易来说, 面对

区块链技术必须权衡的“三元悖论” (即扩展性、去中心化程度和安全性难以同时最大化), 首要任务在于确保贸易数据能够在安全的前提下实现共享和交换[10].

2.2 区块链在数据安全共享与访问控制研究现状

区块链具有去中心化的优势, 其与访问控制技术相结合对于建立分布式系统和加强系统防护方面有很大帮助. Khan 等人[11]在传统模型 RBAC、MAC 和 DAC 等基础上, 设计了一种基于私有链的方案, 对资源和用户权限进行持续、实时的监控. Lin 等人[12]设计了一种基于区块链的认证安全系统, 利用智能合约来进行请求交互, 未授权的实体无法访问数据原文. Cruz 等人[13]在跨域 RBAC 模型中, 通过智能合约对访问权限进行管理, 实现了一种挑战响应身份验证协议, 可以用于验证用户角色所有权. Zhang 等人[14]借助智能合约技术, 构建了一套适用于物联网环境的访问控制结构. 该结构通过精心配置决策制定、用户注册及权限管理等多个智能合约模块, 成功达成了可靠的分布式访问控制目标. Guo 等人[15]以属性为基础, 提出了一种多授权的访问控制方法, 使用区块链智能合约对属性权威、数据拥有方以及请求方的交互进行控制, 不同的属性权威管理不同的属性, 通过发放令牌的形式进行授权, 请求方若想访问数据, 其令牌数量需达到设置好的策略规定. Jemel 等人[16]提出了一种基于区块链和 CP-ABE 的动态访问控制方案, 方案中引入时间动态属性来控制数据的访问时效, 只有属性符合策略要求且在有效时间内的用户才有权利访问数据. Wang 等人[17]探讨了一种应用于去中心化存储体系的数据存储与共享方案, 并创新性地构建了一个融合了去中心化存储架构、以太坊区块链技术以及属性基加密方法的综合框架.

综上所述, 上述方案主要集中在利用区块链构建分布式存储和共享系统, 大部分学者主要针对数据存储共享、访问授权方面进行研究, 但是对用户属性进一步划分、提高共享效率方面等研究较少.

3 方案相关技术

3.1 密文策略属性加密算法 (CP-ABE)

在 CP-ABE 中, 用户权限通过一组属性进行精细描绘, 并且数据提供者负责设定一套基于属性的密文访问规则, 以此判定哪些用户具备解密特定密文的资格. 在这个框架下, 用户的私钥与一组特定属性紧密绑定, 仅当用户的属性集合与待解密密文所指定的访问策略严格匹配时, 该用户才具备成功解密该密文的能力[18,19]. 下面简单介绍 CP-ABE 的 4 种算法.

(1) 系统初始化算法: 输入隐式安全参数 u, 输出公共参数 PK 和主密钥 MK.

$$Setup(u) \rightarrow (PK, MK)$$

(2) 密钥生成算法: 输入主密钥 MK 和描述密钥的属性集合 S, 输出私钥 SK.

$$KeyGen(MK, S) \rightarrow SK$$

(3) 加密算法: 输入 PK, 消息 M 和访问结构 A, 产生密文 CT.

$$Encrypt(PK, M, A) \rightarrow CT$$

(4) 解密算法: 输入 PK、密文 CT、私钥 SK, 私钥由属性集合生成, 输出消息 M.

$$Decrypt(PK, SK, CT) \rightarrow M$$

3.2 区块链与智能合约

区块链是一种分布式数据库技术, 用于记录和存储交易和数据. 它的分布式和不可篡改的特性使得区块链数据的可信度非常高, 适用于各种需要安全可信交易记录的场景[20,21]. 而智能合约则是区块链上的自动化合约, 它是预先定义的代码逻辑和条件, 可以在区块链网络中执行, 与区块链的数据和状态进行交互, 交互图如图 1 所示. 智能合约可以自动执行其中设置的规则和条件, 无需第三方干预, 从而实现了流程的自动化. 区块链和智能合约的结合, 为许多领域带来了新的技术创新[22].

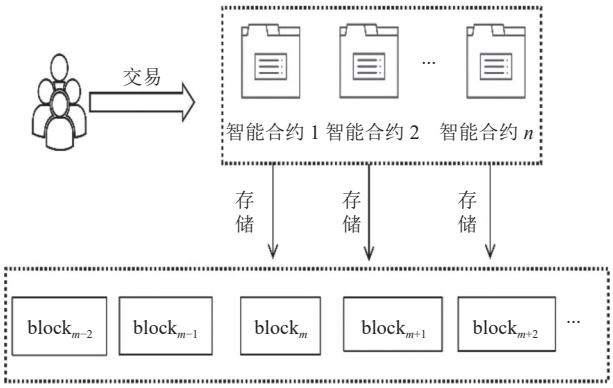

图 1 区块链与智能合约交互图

3.3 星际文件传输系统 (IPFS)

IPFS 是一个点对点的分布式文件系统, 旨在创建

持久且分散的存储和共享方法. 它不依赖于中心化的服务器, 而是使用点对点的协议来分发和分享文件. 并使用内容寻址来标识和检索文件, 每个文件都有一个唯一的哈希地址, 这意味着无论文件保存在网络中的哪个位置, 只要内容不变, 它们的地址都是相同的[23]. IPFS 的分布式存储特性和区块链的去中心化特性相互补充, 通过将文件存储在 IPFS 网络上, 并将文件的地址记录在区块链, 可实现去中心化的文件存储, 提供更高的可用性和稳定性[24].

4 模型介绍

模型一共分为 5 个部分, 分别是 DO (数据所有者, data owner)、DU (数据使用者, data user)、CA、区块链、IPFS, 模型图如图 2 所示.

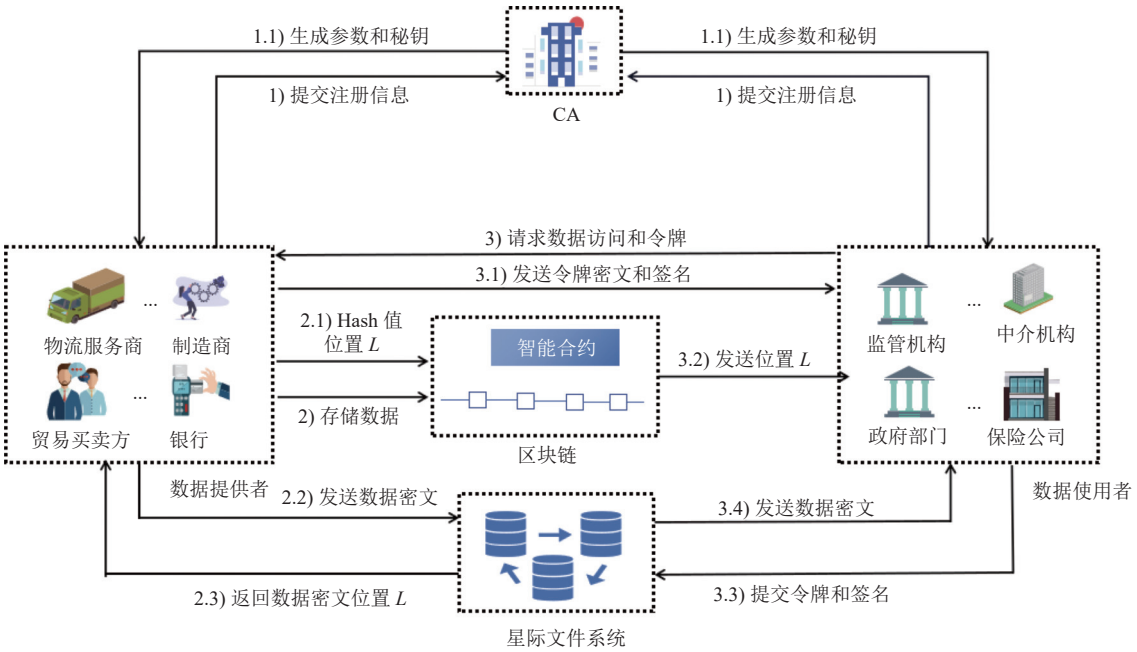

图 2 基于区块链的跨境贸易数据共享与访问控制模型

CA: 是一个权威的且受信任的第三方, CA 负责验证用户的身份信息, CA 根据数据用户的属性生成系统公共参数、全局公钥、主密钥以及和用户属性密切相关的私钥.

DO: 是跨境贸易过程中产生并提供数据的主体, 在跨境物流场景中, 可以是银行、物流服务商、制造商等. DO 根据属性定义访问控制策略, 仅当用户属性满足原 DO 设定的访问策略时, DO 才能够访问相关数据.

DU: 是申请使用数据的用户, DU 可以是政府部门、保险公司、中介机构、海关等. 当然, DU 同时也可以是 DO. 只有当 DU 满足访问控制策略时, DU 才能解密令牌.

区块链: 采用联盟链形式, 所有用户加入都需要经过认证, 增强监管性. 鉴于联盟链存储所有数据的成本和压力, 其仅存储数据的 Hash 值、密文的存储位置. 智能合约为用户提供数据存储、令牌验证和数据禁用等功能, 使用户在数据中的一切行为都被可靠的记录下来, 从而确保数据的安全性和可追踪性.

IPFS: 负责存储 DO 上传的数据, 并返回密文存储位置 L 作为 DU 访问相应数据的索引.

5 方案设计

5.1 双密钥回归模型

双密钥回归模型最早由 Shafagh 等人提出[25], 它使用哈希函数将开始时间和结束时间分别进行多次哈希操作, 将每次哈希的结果作为链中的节点, 并形成一条哈希链, 一条链从开始时间开始, 向后延伸; 另一条链从结束时间开始, 向前延伸. 在所定义的有效时间窗口内, 每个哈希值都是一个有效的密钥. 如图 3 所示, 随机种子为 s_1, 哈希链长度为 N, 由哈希函数按顺序生成哈希令牌从而形成哈希链. 由于哈希函数的不可逆性和抗碰撞性质, 使得无法通过中间节点的哈希值来逆

推开始时间和结束时间的具体数值. 即使攻击者获取了哈希链中的节点信息和哈希值, 也无法直接知道链中的其他节点的原始数据.

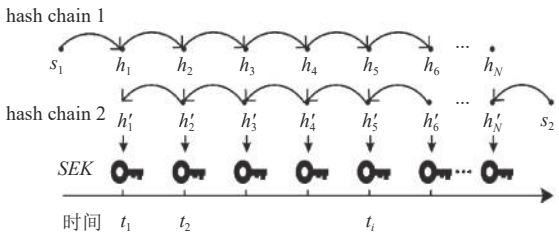

图 3 双密钥回归模型

通过两条相反的哈希链, 我们可以定义开始时间和结束时间, 以限制数据的范围. 例如, 给定时间 (t_4, t_6), 和对应的哈希令牌h_4和h_6, 我们容易计算出 (t_4, t_6)之间的哈希令牌, 但是计算 (t_4, t_6)时间范围外的哈希令牌是十分困难的. 对时间间隔 (t_i, t_j), 计算密钥公式为$SEK_{(i,j)} = KDF\left(h_i \| h'_j\right)$, KDF 为密钥推导函数. 基于此, 可以将密钥的生效时间作为开始时间t_i, 失效时间作为结束时间t_j, 我们只需拥有t_i, t_j对应的哈希令牌对, 就能计算出 (t_i, t_j)所有哈希令牌以及密钥, 从而验证密钥是否处于有效时间范围内. 这种方法提供了一种安全的方式来管理密钥的生命周期, 限制了对设定时间范围外的数据访问.

5.2 访问控制流程设计

首先, DO 和 DU 向 CA 提交注册信息, CA 通过系统初始化算法 $setup(u)$ 生成系统公共参数 PP, 全局公钥 GK 和主密钥 MK. 接下来我们分为 4 个步骤详细阐述方案的设计.

5.2.1 密钥生成设计

Step 1: CA 通过执行算法 $PSkeyGen$ 为每个 DU 生成公私钥对 PK 和 SK.

Step 2: CA 通过执行算法 $SignKeyGen$ 为每个 DU 生成签名公私钥对$\left(\widehat{PK},\widehat{SK}\right)$.

Step 3: 以 DU 的属性集合 S 为基础, CA 通过执行算法 $SKGen$ 为其生成私钥SK'.

5.2.2 数据存储设计

数据拥有者根据本次跨境贸易的时间跨度设置数据被存储周期, 在跨境贸易场景中, 时间跨度为下单时间至确认收货周期, 本文以在该时间跨度内, 监管机构查验出口企业商品原产地证明为例进行详细阐述. 设下单时间为t_{start}, 确认收货时间为t_{end}, 使得$t_{\text{end}} = t_{\text{start}} + N \cdot t_{\text{unit}}$, 记$(t_{\text{start}}, t_{\text{end}}, t_{\text{unit}})$为$\mathcal{T}$.

Step 1: 出口企业执行数据加密算法 $DataEnc(1^{\lambda}, data, PP, T)$ 对于每个时间间隔t_i, 原产地证明数据的哈希摘要和密文计算如下:

$$dig_{data} = H_1(data_i), C_{data} = Enc_k(data_i),\ i \in \{1, \cdots, N\}$$

Step 2: 出口企业执行密钥封装算法 $KeyEncap(\mathcal{T}, \mathcal{K}, PP)$, 即均匀随机地选择两个不同的随机数$s_1, s_2 \in \{0,1\}$用于生成两条反向哈希链的种子. 在抗碰撞的函数的作用下, 对于每个时间间隔t_i, 都会分别生成哈希令牌h_i和h'_j. 接着利用伪随机函数 F 计算出$SEK_i = F\left(\left(h_i \| h'_i\right) \oplus \gamma\right)$. 最后使用 AES 算法$C_{k_i} = Enc_{SEK_i}(k_i), \forall i \in \{1, \cdots, N\}$来包装对称密钥.

Step 3: 出口企业将密文$\tilde{C} = C_{k_i} \| C_{data}$发送到 IPFS, IPFS 存储密文后, 将会向其返回密文位置 L. 最后出口企业通过调用智能合约将位置 L、Hash 值等发布到链上.

5.2.3 令牌生成设计

Step 1: 当监管机构需要查验在时间t_i到t_j之间的跨境贸易数据时, 它发送请求信息$R = \left(uid, \text{DO}_{uid}, \left(t_i, t_j\right)\right)$给出口企业, 出口企业通过调用禁用合约验证其是否具有访问权限, 如果具有权限, 则执行以下步骤.

Step 2: DO 通过 $Token\left(\gamma, \widehat{SK}, R, \mathcal{HL}\right)$算法生成令牌 T, 其中令牌 T 包含了令牌头和令牌体部分. 令牌头分为 id (令牌标识)、$time$ (有效时间)、num (可用次数)、 $user$ (使用者)、 $parent$ (父令牌 id)、son (子令牌 id) 这 6 个字段. 令牌体则包含一个随机数、DO 的身份标识 DO_{uid}、哈希令牌h_i和h'_j以及对这 4 个成分的签名 sig, 令牌结构如图 4 所示. 接下来出口企业对整个令牌进行签名.

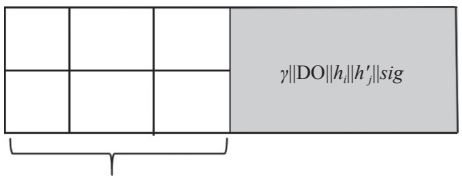

图 4 令牌体结构

Step 3: 出口企业执行 $TokenEnc(PP, GK, (M, \rho), T)$ 算法来加密令牌, 其中 (M, ρ) 为其自行定义的访问制策略, 并将加密后的密文 C 发送给监管机构. 如果监管机构的属性集 S 满足访问控制策略, 那么其就可以使用属性私钥SK'来解密密文 C, 并得到访问令牌 T.

5.2.4 数据访问设计

监管机构首先发送请求$R=\left(uid,\mathrm{DO}_{uid},\left(t_i,t_j\right)\right)$至区块链, uid 为其自身身份标识, 随后区块链将向其返回数据存储位置 L, 根据位置 L, 将对应令牌 T 及其签名 S_T 发送至 IPFS. 接下来调用验证合约对令牌进行验证, 验证成功后, IPFS 将时间t_i和时间t_j之间的对应密文流 $\tilde{C}$发送至监管机构并通过执行 $DataDec(T, PP, \tilde{C})$ 算法来获取跨境贸易数据 $data$, 算法描述如下.

(1) 从令牌 T 中提取h_i, h'_j和λ.

(2) 对任意$\forall\varepsilon\in[i,j]$, 计算$h_\varepsilon=H_1^{\varepsilon-i}(h_\tau)h'_\varepsilon=H_1^{j-\varepsilon}\left(h'_j\right)$, $SEK_\varepsilon=F\left(\left(h_\varepsilon\parallel h'_\varepsilon\right)\oplus\gamma\right)$, $k_\varepsilon=Dec_{SEK_\varepsilon}$.

(3) 对任意$\varepsilon\in[i,j]$, 计算$data_\varepsilon=Dec_{k_s}(C_{data_s})$得到明文的跨境贸易数据.

最后, 监管机构调用数据验证合约验证数据完整性以及是否被篡改.

5.3 智能合约设计

通过智能合约, 贸易参与方可以自主管理数据, 并通过合约规定的条件和权限进行数据的存储、验证、禁用操作. 通过发起对 event 的调用来触发相应的事件响应, 并将事件预先设定的各项参数载入交易日志中, 便于后期的查阅和追踪. 当智能合约的状态经历变更时, 相关的调用详情将会被整合为一笔交易记录, 并永久存储于链上, 合约主要提供以下 4 个接口.

数据存储: 该功能由出口企业执行, 它通过在链上发布数据 Hash 值和存储位置, 使监管机构能够更容易对相关数据进行检索. 在该流程中, msg sender 代表出口企业地址. 当出口企业发布的数据与链上数据重合, 数据发布将会失败, 相关算法如算法 1 所示.

算法 1. 数据存储算法

输入: *hash* 值、密文位置 *L*、定价 *price*.
输出: bool 值.

```
1. get datas.length len
2. for i←0 to len–1 do
3.     if datas[i].Hash == hash then
4.         return false
5.     end if
6. end for
7. datas.add(hash, L, price, msg.sender, now)
8. return true
```

令牌验证: 该功能由监管机构执行. 监管机构通过提交令牌 T、令牌签名、公私钥等来验证令牌的有效性. 如果提交的令牌数据与元数据一致, 则验证成功, 否则验证失败, 相关算法如算法 2 所示.

算法 2. 令牌验证算法

输入: 令牌 T、令牌签名S_T、系统公共参数 PP、DU 签名公钥$\widehat{PK}$.
输出: bool 值.

```
1. verify←1
2.     if (H0(g^α·PK^−r,T)=r)∧(H0(γ||DO_uid||h||h'_i)=r')
3.         return true
4.     end if
5. return false
```

数据验证: 该功能由监管机构执行. 在该合约中, 位置 L 和 Hash 值将会被比对验证, 从而确保数据完整性且未被篡改. 当数据一致时, 则验证成功, 否则验证失败, 相关算法如算法 3 所示.

算法 3. 数据验证算法

输入: 密文存储位置 *L*, 数据哈希摘要 dig_{data}.
输出: bool 值.

```
1. get datas.length len
2. for i←0 to len–1 do
3.     if datas[i].Cid == L and dig_datas == H1(datas) then
4.         return true
5.     end if
6. end for
7. return false
```

数据禁用: 该功能由出口企业执行. 当非法用户请求访问时, 出口企业通过将非法用户地址添加到禁用列表, 进而阻止其继续访问, 保护数据安全, 相关算法如算法 4 所示.

算法 4. 数据禁用算法

输入: 非法访问用户地址 (*du*).
输出: bool 值.

```
1. get datas.length len
2. for i←0 to len–1 do
3.     if datas[i].datasOwner == msg.sender and dl not in datas[i].
forbidList then
4.         add dl to datas[i]
5.         return true
6.     end if
7. end for
8. return false
```

6 模型分析

6.1 安全性分析

本文主要从令牌安全性和数据安全性两方面进行分析, 具体如下.

6.1.1 令牌安全性

当某些用户试图非法获取跨境贸易数据时, 他们可能会与其他用户共谋, 以获取有效的秘密数λ或交换哈希令牌h_i和h'_j. 在我们所提出的令牌结构中, 令牌体的签名是至关重要的, 一旦令牌被篡改, 签名验证就会失败. 此外, 对于每个完整的令牌, 其签名还可以用于进一步确保令牌的不可伪造.

6.1.2 数据隐私安全

在本文提出的方案中, 数据提供者使用了 CP-ABE 加密技术来共享数据, 而 CP-ABE 的安全性对于数据的隐私保护至关重要. 为了分析方案的安全性, 我们考虑了明文攻击的情况. 由 1 个挑战者和 1 个概率多项式时间 (PPT) 攻击者组成的安全游戏的定义如下.

初始化: 挑战者执行 *Setup* 算法, 将系统公共参数 PP 发送给攻击者.

阶段 1:

(1) 攻击者发送一个消息 m 给挑战者, 挑战者通过数据加密算法 *DataEnc* 生成密文C_m并发送给攻击者.

(2) 挑战者通过密钥封装算法 *KeyEncap* 生成密文C_k并发送给攻击者.

挑战: 挑战者收到来自攻击者的两条等长消息m_0和m_1, 并从m_0和m_1里随机选择m_b ($b \in \{0,1\}$), 最后执行 *DataEnc* 和 *KeyEncap* 算法生成C_k和C_{m_b}, 并将$C_k \| C_{m_b}$发送给攻击者.

阶段 2: 攻击者重复阶段 1 的操作.

猜测: 攻击者猜测一个数字b'代表 b.

在上述游戏中, 攻击者优势定义为$Adv_A^{\text{cpa}} = |\Pr[b = b'] - 1/2|$, 其优势几乎为 0, 因此我们可以得出本方案能够抵御明文攻击.

6.2 实验与仿真分析

为了衡量本文所提方案性能, 我们对智能合约开销进行测试并对主要算法进行性能分析, 分析所提方案的存储和计算成本. 操作系统为 Ubuntu 18.04, 处理器为 Intel(R) Core(TM) i5-8250U@1.60 GHz, 内存为 8 GB. 智能合约利用 Solidity 开发, 区块链平台选择以太坊, CP-ABE 方案选择 PyCharm 第三方库实现.

6.2.1 智能合约分析

合约在执行过程中, 不同的合约往往需要消耗不同的资源. 在以太坊内, Gas 充当交易与智能合约执行必需的计算与交易成本. 为量化合约执行时 Gas 的消耗量, 我们采取的步骤是运用 Remix 工具逐个执行合约函数来进行计算, 图 5 展示了测试结果中 Gas 的消耗情况.

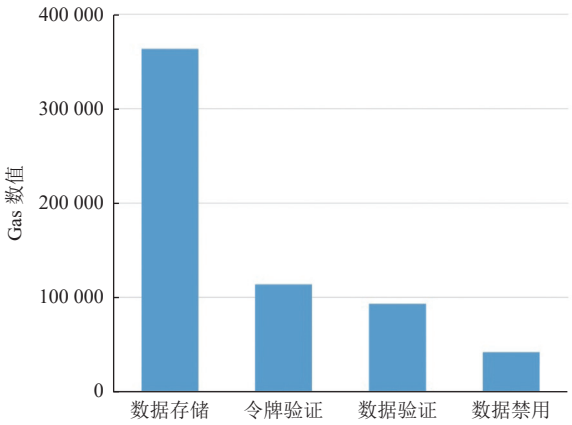

图 5 合约函数 Gas 消耗情况

图 5 结果表明数据存储合约消耗 Gas 的数量最多, 因为在数据存储合约运行时, Hash 值、位置 L 将会被逐一对比和检查后再发布到链上, 故消耗 Gas 数量最多. 其他合约消耗 Gas 数量较少, 均远低于数据存储合约的 Gas 消耗值.

6.2.2 主要算法测试分析

我们对几个重要算法进行测试以获得系统各阶段的时间开销, 每个算法进行 10 次测试, 最终结果取其平均值. AES 算法和 RSA 算法因其具有成熟性和高效性, 不在我们的测试范围内. 实验设置存储阶段哈希链长度为 1 000, 属性数量为 4, 数据大小为 5 MB. 实验结果如图 6 所示.

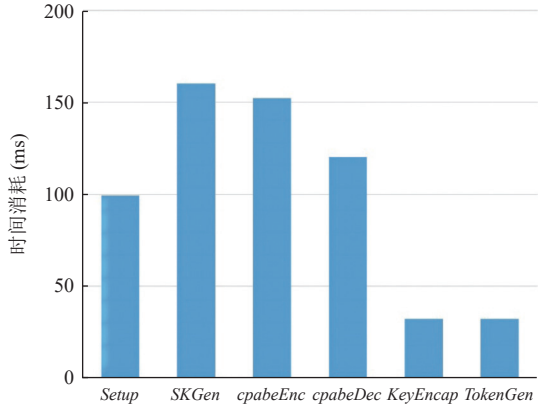

图 6 各阶段时间开销

图 6 第 1、2 列分别表示系统初始化和密钥生成所需时间, 在我们的设计方案中, 系统初始化只发生一次, 在访问控制策略不变的情况下, 同样只需要为 DD 生成一次密钥. 第 3、4 列表示了 CP-ABE 加解密所需

时间, 第 5 列为密钥封装算法所需时间, 最后一列为令牌生成算法执行所需时间.

我们还通过对不同长度哈希链进行测试, 进而了解哈希链长度对密钥封装 (*KeyEncap*) 操作所需时间开销的影响程度, 实验结果如图 7 所示. 可以观察到随着哈希链长度的增加, *KeyEncap* 的时间成本呈线性增加趋势. 当哈希链长度达到 1 000 时, *KeyEncap* 的时间成本仅在 0.1 s 以下. *KeyEncap* 在本方案中只执行一次, 除非在一次访问结束后系统部分更新密钥. 尽管时间成本呈线性增加, 但对于常见的哈希链长度, 密钥封装的时间成本仍然非常低.

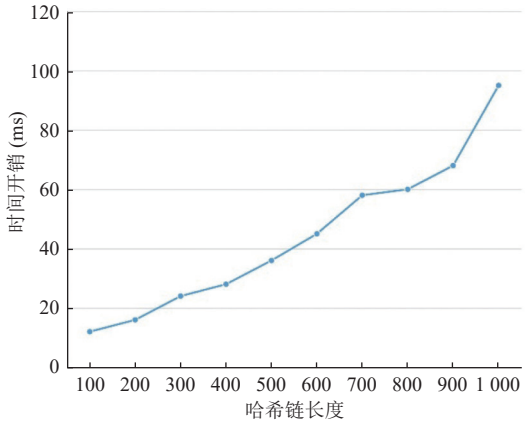

图 7 *KeyEncap* 的时间开销

图 8 展示了 CP-ABE 在处理不同数量属性时, 执行加解密操作时间消耗的变化趋势, 设数据恒定为 5 MB. 从图中观察到, 加解密操作的耗时与访问策略中属性的数量呈正相关: 属性数量的增加, 加解密过程中计算任务和操作步骤增多, 进而导致整体处理时间的增长.

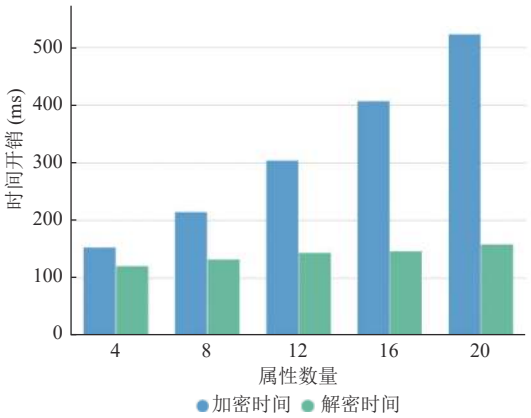

图 8 CP-ABE 在不同属性数量下的时间开销

图 9 展示了 CP-ABE 加密算法在不同数据容量下的运行时间消耗情况, 其中属性数量被设定为固定的 4 个. 由于本方案采用 CP-ABE 加密, 访问策略涉及 4 个属性, 在跨境贸易中, 主要涉及物流信息、货物单证等信息的共享, 一般数据不会太大. 因此, 在数据容量不超过 10 MB 的情况下, 其加解密处理时间能够保持在低于 240 ms 和 160 ms 的水平. 尽管相较于传统的对称加密方法, CP-ABE 加解密耗时更长, 但鉴于其能有效地实现在多个用户间进行细粒度访问控制, 显著增强数据共享过程中的安全性, 故而承受这一适度增加的时间成本是合理的.

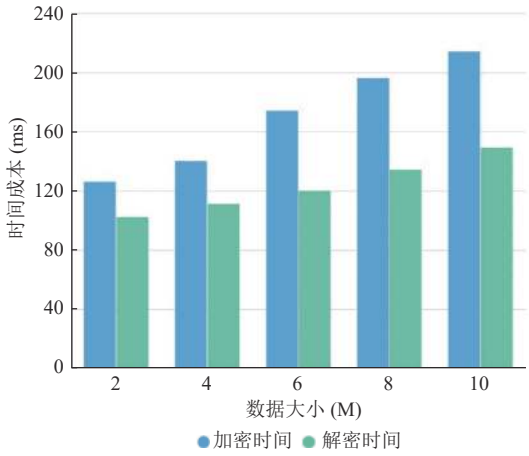

图 9 CP-ABE 在不同数据大小下的时间开销

6.3 功能对比分析

将本方案与区块链和数据共享及访问控制结合领域的几个方案[12,16–18]做了功能上的对比, 结果如表 1 所示.

表 1 不同方案功能对比

指标	文献[12]	文献[16]	文献[17]	文献[18]	本文
时间维度访问控制	×	×	√	×	√
数据完整性验证	×	×	×	√	√
数据访问权限撤销	×	×	√	√	√
数据共享	√	√	√	√	√
智能合约	√	√	×	×	√
隐私保护	√	√	√	√	√

通过分析各项指标发现, 本方案支持通过时间维度对访问权限进行划分, 实现更细粒度的访问控制, 还支持根据链上记录验证数据的完整, 同时, 通过智能合约实现了数据验证以及访问权限禁用等功能. 与其他方案相比, 本方案具有一定优势.

7 结束语

本文针对跨境贸易活动中存在数据安全、信息不对称等问题, 提出了一种基于区块链的数据共享与访

问控制方案. 通过将区块链和 IPFS 结合, 以平衡和缓解区块链本身的存储压力, 保障数据的安全性. 利用双密钥回归模型提供安全的方式来管理密钥的生命周期, 限制了对设定时间范围外的数据访问. 此外, 设计相应智能合约从而达到对数据流转过程中的精细化管理, 以实现对链上数据的有效监管与控制, 提升共享效率, 从而推动数据的可信、公开及共享化进程. 在后续的工作中, 我们将在此基础架构上进一步拓展数据确权功能, 旨在深度保障数据所有者的权益, 有力驱动数据的安全共享与价值释放.

参考文献

1 2022 年我国外贸进出口规模再创历史新高. 中国新闻发布 (实务版), 2023, (2): 51.

2 国务院办公厅印发《关于推进对外贸易创新发展的实施意见》. 军民两用技术与产品, 2020, (12): 6.

3 王亚平. 贸易数字化与数字强贸——《“十四五”对外贸易高质量发展规划》有关内容解读. 国际商务财会, 2021(18): 3–5, 14.

4 魏星, 唐剑. 探究对外贸易企业数字化转型的机制及优化路径. 全国流通经济, 2021(30): 33–35.

5 王爽, 贺群舟, 邢国繁. 基于区块链技术的新型跨境贸易体系构建研究. 商业经济研究, 2024(2): 142–145.

6 吴花平, 刘自豪. 基于区块链加密技术的云会计数据安全探究. 重庆理工大学学报 (社会科学), 2024, 38(2): 96–105.

7 Razon AK. Liberalising blockchain: An application of the ‘GATS’ digital trade framework. Melbourne Journal of International Law, 2019, 20(1): 125–157.

8 工业和信息化部信息中心. 2018 年中国区块链产业白皮书. 北京: 工业和信息化部信息中心, 2018.

9 上海区块链技术与应用白皮书编写组. 2019 上海区块链技术与应用白皮书. 上海: 上海区块链技术与应用白皮书编写组, 2019.

10 于涛, 姚凡军, 高红伟. 区块链数字生态系统赋能跨境贸易中的博弈问题研究. 运筹与管理, 2023, 32(11): 233–239.

11 Khan MY, Zuhairi MF, Ali T, *et al*. An extended access control model for permissioned blockchain frameworks. Wireless Networks, 2020, 26(7): 4943–4954. [doi: 10.1007/s11276-019-01968-x]

12 Lin C, He DB, Huang XY, *et al*. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of Network and Computer Applications, 2018, 116: 42–52. [doi: 10.1016/j.jnca.2018.05.005]

13 Cruz JP, Kaji Y, Yanai N. RBAC-SC: Role-based access control using smart contract. IEEE Access, 2018, 6: 12240–12251. [doi: 10.1109/ACCESS.2018.2812844]

14 Zhang YY, Kasahara S, Shen YL, *et al*. Smart contract-based access control for the Internet of Things. IEEE Internet of Things Journal, 2019, 6(2): 1594–1605. [doi: 10.1109/JIOT.2018.2847705]

15 Guo H, Meamari E, Shen CC. Multi-authority attribute-based access control with smart contract. Proceedings of the 2019 International Conference on Blockchain Technology. Honolulu: ACM, 2019. 6–11.

16 Jemel M, Serhrouchni A. Decentralized access control mechanism with temporal dimension based on blockchain. Proceedings of the 14th IEEE International Conference on e-Business Engineering (ICEBE). Shanghai: IEEE, 2017. 177–182.

17 Wang SP, Zhang YL, Zhang YL. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. IEEE Access, 2018, 6: 38437–38450. [doi: 10.1109/ACCESS.2018.2851611]

18 Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Taormina: Springer, 2011. 53–70.

19 黄锦. 云计算下 CP-ABE 访问控制方案研究 [硕士学位论文]. 桂林: 桂林电子科技大学, 2019.

20 张建标, 张兆乾, 徐万山, 等. 一种基于区块链的域间访问控制模型. 软件学报, 2021, 32(5): 1547–1564. [doi: 10.13328/j.cnki.jos.006011]

21 郭上铜, 王瑞锦, 张凤荔. 区块链技术原理与应用综述. 计算机科学, 2021, 48(2): 271–281.

22 袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, 42(4): 481–494.

23 Benet J. IPFS-content addressed, versioned, P2P file system. arXiv:1407.3561, 2014.

24 史爱武, 付科巽, 魏银珍, 等. 一种基于区块链与 IPFS 的医疗数据共享模型. 软件导刊, 2023, 22(5): 109–114.

25 Shafagh H, Burkhalter L, Ratnasamy S, *et al*. Droplet: Decentralized authorization and access control for encrypted data streams. Proceedings of the 29th USENIX Security Symposium. USENIX Association, 2020. 2469–2486.

(校对责编: 张重毅)