基于主从多链的科学数据共享方法构建与实证研究

陈　俊[1,2,3]，杨　锐[1,3]，李岚春[1,3.4]，周子健[1,2,3]

（1. 中国科学院武汉文献情报中心，湖北　武汉　430071；2. 中国科技云武汉区域中心，湖北　武汉　430071；
3. 科技大数据湖北省重点实验室，湖北　武汉　430071；4. 中国科学院大学　经济与管理学院，北京　100190）

摘　要：针对当前科学数据管理中普遍存在安全性不足的问题，试图基于主从多链理论，探索提出一套科学数据保护与共享架构方法。提出一种基于主从多链的科学数据保护与共享方法，这一方法借助多个智能合约、数字签名、星际文件系统（IPFS）技术，并结合科学数据的分级分类和身份认证实现细腻度管理；采用主从多链结合的方式，确保数据的安全性和可扩展性。实证研究结果表明，本方法在存储开销方面显著优于公共链方案，在性能上提升约 3 倍，并在处理大量交易时展现出更高的稳定性与可靠性。综上所述，该方法具备去中心化、安全可靠、不可篡改等重要特性，能够有效应对日益增长的科学数据保护与共享需求。

关键词：区块链；科学实验数据；数据安全；智能合约；访问控制

中图分类号：TP309. 7；TP311. 1　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2024. 11. 010

引用格式：陈俊，杨锐，李岚春，等. 基于主从多链的科学数据共享方法构建与实证研究［J］. 网络安全与数据治理，2024，43(11)：56 - 63.

Construction and empirical research on scientific data sharing method based on master-slave multi-chain

Chen Jun[1,2,3]，Yang Rui[1,3]，Li Lanchun[1,3.4]，Zhou Zijian[1,2,3]

（1. Wuhan Library，Chinese Academy of Sciences，Wuhan 430071，China；
2. Wuhan Regional Center，China Science and Technology Cloud，Wuhan 430071，China；
3. Hubei Key Laboratory of BigData in Science and Technology，Wuhan 430071，China；
4. School of Economics and Management，University of Chinese Academy of Sciences，Beijing 100190，China）

Abstract：In response to the common issue of insufficient security in current scientific data management，this paper attempts to explore and propose a set of scientific data protection and sharing architecture methods based on the master-slave multi-chain theory. This paper proposes a scientific data protection and sharing method based on the master-slave multi-chain concept. This method utilizes multiple smart contracts，digital signatures，and the InterPlanetary File System（IPFS）technology，combined with the grading and classification of scientific data and identity authentication to achieve fine-grained management；it adopts a master-slave multi-chain combination to ensure data security and scalability. The empirical research results show that this method significantly outperforms public blockchain solutions in terms of storage overhead，with approximately a threefold improvement in performance. It also demonstrates greater stability and reliability when processing large volumes of transactions. In conclusion，this method possesses key characteristics such as decentralization，security，and immutability，making it highly effective in addressing the growing demand for scientific data protection and sharing.

Key words：blockchain；scientific experimental data；data security；smart contract；access control

0　引言

由于参与人员多、数据类型多样、生成时机和环境的特殊性以及不同程度的保密需求，科学实验数据管理面临复杂性，科研机构和个人通常因为知识产权保护的顾虑，往往不愿意立即公开实验数据，这导致了数据开放的困难[1]。为解决数据可信度和准确性，学术界和行

业界进行深入研究，并涌现出云储存等多类型技术方案，但未能有效破除科研机构之间的数据共享问题。相较之下，区块链技术凭借其去中心化、不可篡改和安全可信的特质[2]，被视为解决数据安全和共享问题的有力工具。

本文设计了一种基于主从多链的科学数据保护和共享系统。通过细分授权和数据分级，提高交易处理速度，优化数据管理。系统利用智能合约和数字签名，建立了科研机构间的数据共享和信任机制。结合 IPFS 技术[3]，减少链上交易成本，加快数据访问和验证速度。系统采取了身份验证、加密和数据保护等措施，以降低风险并保障通信安全。这有助于科研人员和机构高效、安全地共享数据。

1 文献综述

区块链因其不可篡改、可溯源等优良特性而被广泛使用。文献［4］针对区块链吞吐量限制以及单链存储效率低下等问题，提出基于多链架构的 BlockTrail，并应用于溯源场景。结果证明，该区块链性能优于传统单链结构，但由于节点需要维护账本一致性使其存储开销仍然较大。文献［5］设计了一种多区块链架构，以实现链间互操作性并提高事务吞吐量。但该架构的数据存储效率需优化，以减少冗余和避免对低敏感性数据的存储浪费。文献［6］构建了基于多层次区块链的医疗数据共享模型，IPFS 用于保存加密的健康数据以及诊断数据，IPFS 的唯一性使得数据安全性得到保障，但多层区块链的交互使得系统开销较大。文献［10］提出 BC-Store 框架，通过将区块链数据分类并分布式存储于链上和 IPFS 上，有效减少了存储需求。尽管该方法减轻了链上存储的压力，但确保细粒度数据安全的问题仍待解决。文献［13］构建基于主从多链的数据分类分级访问控制模型，通过 MCLP-RBAC 访问控制可以实现细粒度的数据安全存储与保障，但没有考虑到数据分享者所在机构对数据的管理授权以及数据分享收益确权。

在日益复杂繁多的信息资源环境下，多分类数据的隐私级别和重要性差异巨大，确保数据权益成为一个重要问题[12]。本文针对数据分类分级保障，结合侧链和 IPFS 链下扩容方案[11]，设计提出了基于主从多链的数据分类分级访问控制模型。通过主从多链的形式来实现数据分类[15]，同时结合 IPFS 以获得更佳的扩容效果，以有序存储各类大量数据；构建分级访问控制模型，以实现链上链下数据的细粒度管理；将访问控制策略部署在智能合约中，从而实现权限的动态管理。

2 基于主从多链的数据共享方法构建

2.1 整体架构

为了更好地应对数据分类分级存储，保障不同敏感程度数据的安全性，本文引入联盟链（hyperledger fabric）技术，构建基于主从多链的数据分类分级访问控制模型，如图 1 所示。该模型由参与主体、区块链网络和 IPFS 三部分构成。

2.1.1 参与主体

参与主体由科研工作者、管理人员、科研机构组成。

（1）科研工作者在整个系统中是数据提供与获取的角色，有权对自己拥有的数据进行分级分类的管理，并授权对应级别的用户进行访问，并将原始数据上传至 IPFS[7]。

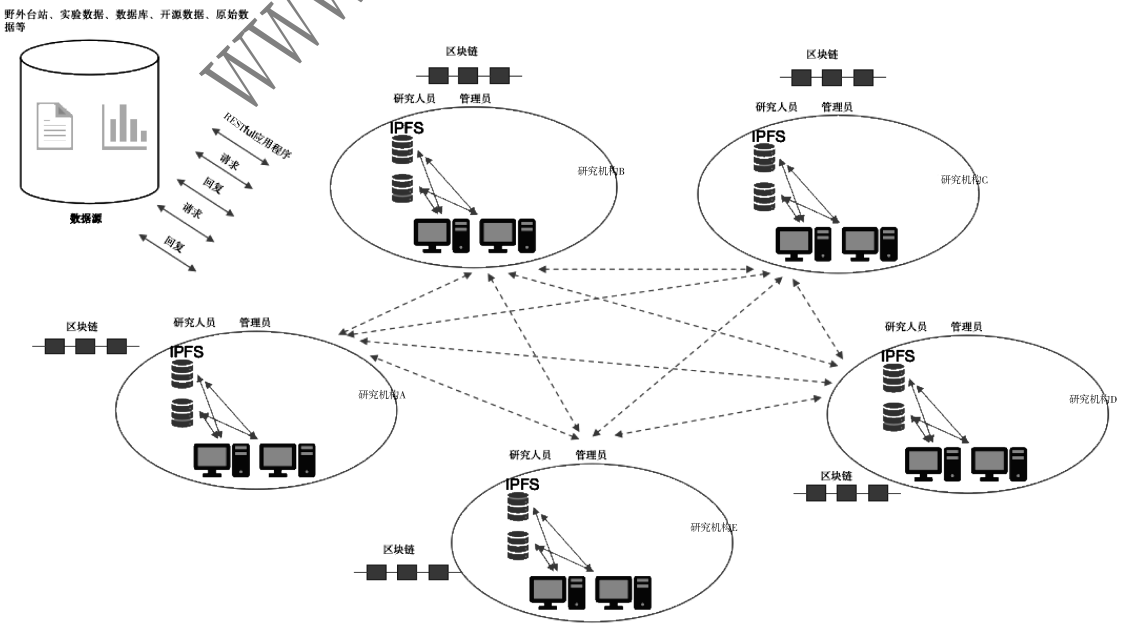

图 1 科学数据共享整体架构

（2）管理人员在整个系统中是数据管理的角色，制定和实施数据分级分类管理政策[8]，分配科研资源，帮助科研工作者有效地使用数据和相关工具。

（3）科研机构拥有对科研工作者的数据审核安全监管、激励手段策略制定。

2.1.2 区块链网络

本文区块链网络由一条主链和多从链组成。

（1）主链网络层负责用户身份的验证和精确的权限分配。每位用户都拥有独特的身份标识和特定的权限等级，如读、写、编辑或删除。用户根据角色和组织分配到不同的权限类别，并依据精细的访问控制策略与数据资源相连，确保只有授权的个体能够访问他们被允许的资源。

（2）从链网络层处理通过主链验证的信息和记录数据的 IPFS 哈希值[9]。当 IPFS 上添加新数据时，从链记录数据哈希和元数据，包括权限等级和访问控制策略。从链还负责定期校验 IPFS 数据的完整性，保障数据未遭篡改。若发现数据异常，从链将启动恢复机制，从备份或其他来源重取数据并更新哈希值。

2.1.3 分布式存储

引入 IPFS 支持原始数据存储，同时将 IPFS 返回的哈希值及其他元信息回传至链上，从而构建一个链上链下协同存储的模式，其主要特点包括：

（1）去中心化存储：提高数据的可靠性和抗篡改性，因为即使某些节点受到攻击或故障，数据仍然可以从网络中的其他节点检索。

（2）高效的数据检索：创新性采用基于内容的寻址，用户可通过数据的哈希值直接检索数据，提高了数据检索的效率和速度。

（3）数据不可篡改：每个文件内容生成一个唯一的哈希值。一旦文件内容发生变化，其哈希值也会随之改变。

（4）支持大规模数据共享：IPFS 可以用来存储大量的科学实验数据，而区块链则用来存储数据的元数据和访问控制信息，确保数据的安全性和可追溯性。

2.2 结构设计

2.2.1 主从多链结构

传统单链结构的吞吐量和存储容量可能会受到限制，因此引入从链结构，从而构建主从多链网络架构，如图 2 所示。

以上面三个机构为例，本文基于联盟链进行主从多链构建。节点（node）分为普通共识节点、通信锚节点和数据交换节点。IPFS 存在于每个机构中，共同组成了一个去中心化分布式存储。图 2 中三个机构的普通共识节点和通信锚节点构成了主链层，普通共识节点、通信锚节点和数据交换节点构成了从链层。

（1）普通共识节点（GeneralConsensus Node，GCN）负责存储整个区块链的副本，验证交易，维护区块链的安全性和一致性，并参与共识过程。普通共识节点在网络中扮演核心角色，确保交易的有效性和一致性，以及参与区块链的共识算法，以共识算法采用 Fabric 本身提供的实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）算法。

（2）通信锚节点（CommunicationAnchor Node，CAN）负责在区块链网络中传输信息，帮助主从链之间进行信息传递，促进网络的连接和通信。通信锚节点负责广播新的交易和区块到网络中的其他节点，确保信息的传递和同步，还有助于节点之间的连接建立和维护。

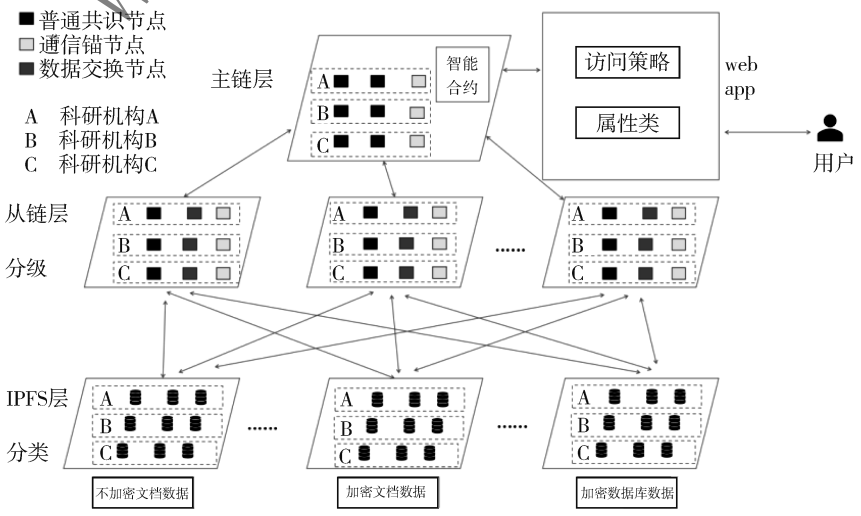

图 2 主从多链结构设计

（3）数据交换节点（DataExchange Node，DEN）分布在从链之上，它允许用户或应用程序根据内容地址或哈希值查询并检索存储在 IPFS 网络中的数据。用户可以通过查询节点来获取特定文件或内容。数据交换节点可以缓存最近访问的数据块，以提高数据的可用性和减少网络负载，有助于提高数据访问的效率。数据交换节点充当用户或应用程序与 IPFS 网络之间的接口，负责将请求传递给其他 IPFS 节点，协调数据的检索和传输。

2.2.2 分级分类存储模式设计

数据分级分类在数据安全治理过程中具有重要意义，科学数据的多样性使得数据管理和分析变得复杂，但也提供了广泛的研究机会和应用潜力。本文借鉴文献［14］4 级数据分类模式：1 级（高度机密的科学数据）、2 级（机密的科学数据）、3 级（有限共享的科学数据）、4 级（开放共享的科学数据），设计提出多从链结构科学数据分级方法，如表 1 所示。

在科学数据分类存储设计中，系统允许科研人员根据数据的保密等级和类型选择相应的存储方式。对高机密数据和机密数据，采取本地存储，不上网仅在系统做存证和版权声明；对有限共享数据，利用 IPFS 分布式加密存储在系统各节点上；对开放共享数据，不加密上传到 IPFS 上开放共享[16]。通过数据分类，可以实现更有效的数据管理和快速的数据检索。利用 IPFS 的 256KB 分块机制，数据被分割成一系列的 256 KB 大小的块进行存储[17]。每个数据块都有一个唯一的哈希值，用于在 IPFS 网络中的定位和检索。IPFS 的分块存储机制具有数据存储的高效性和高可靠性，即使在部分节点失效的情况下，也能从网络中的其他节点检索到数据块，确保数据的完整性和可靠性。

2.2.3 科学数据共享智能合约设计构建

（1）机构共识节点验证智能合约（Institutional Consensus Nodes Validate Smart Contracts，ICNVSC）

表 1 科学数据分级

等级描述	链名称	等级代码	数据类型样本	节点网络	数据存储和传输	访问控制
高度机密的科学数据	高度机密的科学数据链（Chain A）	1	高度机密，绝大多数人无权访问； 高度加密，采用最高级别的安全措施； 严格的身份验证和权限控制； 特殊访问审批程序，需获得高级授权	小	最高级别的加密和安全措施	严格，需要高级别的授权
机密的科学数据	机密的科学数据链（Chain B）	2	需要特定授权才能访问； 有限的权限控制，只有特定人员或组织能够访问； 数据传输和存储采用较高级别的加密	较小	较高级别的加密	严格，但相对较多人员可以获得访问权限
有限共享的科学数据	有限共享的科学数据链（Chain C）	3	有一定的数据共享政策和许可协议； 可以供合作伙伴、特定领域的研究人员或项目组访问； 数据传输和存储采用基本的安全措施	较大	一定政策和许可协议约束	根据共享政策管理，需要适当的许可
开放共享的科学数据	开放共享的科学数据链（Chain D）	4	数据是公开的，没有特定的访问限制； 可以用于科研、教育、创新和公共利益； 数据通常在公共数据存储库中提供，如科研文献数据库、开放数据平台等	公开	无需授权	自由访问

在区块链网络中，机构共识节点验证是一种常见的共识机制，它依赖于预先选定的、信任的机构节点来验证交易和维护区块链的完整性。智能合约可以用来执行和验证各种基于规则的交易。

（2）分级访问权限智能合约（Hierarchical Access Rights Smart Contract，HARSC）

分级访问权限是一种常见的安全措施，用于确保只有具有适当权限的用户能够访问或修改敏感信息。在区块链环境中，可以通过智能合约来实现分级访问权限的管理。描述如下。

在分级访问权限智能合约中定义三种角色：Provider、Requester 和 Admin。创建 assignRole 和 revokeRole 函数以分配和撤销用户角色，并使用修饰符 onlyAdmin 来控制对特定操作的访问。允许在智能合约中创建复杂的权限管理系统，确保只有具有适当权限的用户能够访问敏感操作或数据。

（3）数据激励智能合约（Data Motivates Smart Contracts，DMSC）

数据激励智能合约是一种基于区块链的合约，通过奖励机制激励个人或组织提供和共享数据。首先定义 DMSC 智能合约，该合约包含 DataInfo 结构体用于存储数据的信息，以及 dataInfos 映射表用于索引所有上传的数据。然后创建 uploadData 函数，允许用户上传数据，并保存数据的哈希值和提供者的地址。接着创建 rewardData 函数，允许给定的奖励发送给数据的提供者。

2.3 功能实现

模型共享方案分为用户分级访问控制流程、主从多链用户科学数据共享流程和用户获取激励奖励流程三个阶段。本文将基于科学实验场景下的数据作为原始科学数据，科研机构作为机构参与主体，科研工作者作为数据提供者，其涉及符号如表 2 所示。

2.3.1 参与主体机构认证流程

科研机构在加入整个联盟区块链网络时，需在主链中证明其机构身份的真实性，即在主链中调用 ICNVSC 向其他已经过验证的机构发送请求，当超过一半机构中的 GCN 认同后才可被写入 ICNVSC 中。假设 ICNVSC 中已存在 $2N$ 个 GCN，新的科研机构（简称 MB）进入系统时，首先在区块链网络中的主链通过椭圆曲线加密（ECC）技术生成公私密钥对并生成相应地址，之后通过调用 ICNVSC 将身份信息向区块链网络中已存在的 $2N$ 个 GCN 发起验证交易。所有的 GCN 收到请求后，验证 MB 的身份信息。当 MB 通过 N 个 GCN 验证成功后才可被写入 ICNVSC，并将 MB 中 GCN 和 CAN 加入 MC 中，MB 中 GCN、CAN 和 DEN 加入 SC 中。

表 2　符号说明

符号	含义
MB	主体
NA	节点属性，包括 id、adress、role
Sig（）	数字签名，利用 MB 私钥进行的
MC	主链
SC	从链
PK_{MB}	MB 的 AES-256 公钥
SK_{MB}	MB 用于签名的私钥
Tx	交易信息，包括操作、发送方、接收方等信息
P	用户的访问权限，包括 Read、Write、Download、Upload 权限
H（）	哈希算法，将消息或数据散列为固定长度的值
DataLevel	数据分级权限（1，2，3，4）

2.3.2 主体用户分级访问控制流程

本文主体用户分为科研工作者（researcher）、管理人员（manager），故角色分为科学数据提供者（provider）、科学数据获取者（requester）、科学数据管理员（admin）。数据分级为高度机密的科学数据、机密的科学数据、有限共享的科学数据、开放共享的科学数据。在用户访问数据分级访问的过程中会调用 HARSC。

（1）用户和角色定义：用户集合 U 包含所有参与系统的个体。用户角色通过函数 role：$U\rightarrow$ {"provider","requester","admin"} 来定义。“provider”角色的用户负责上传科学数据。“requester”角色的用户负责从系统中获取科学数据。“admin”角色的用户负责管理系统中的数据，包括数据的分级和分类。

（2）数据属性和分类：数据集合 D 包含所有存储在系统中的科学数据。数据类型集合 T 定义可能的数据类型，如表格、文档、数据库等。数据类型通过函数 type：$\rightarrow$type：$D\rightarrow T$ 来定义。数据安全级别集合 $S=\{1,2,3,4\}$ 定义不同的安全级别，从高到低分别对应高度机密、机密、有限共享、开放共享。数据安全级别通过函数 level：$D\rightarrow S$ 来定义。

（3）访问控制和管理操作：访问权限通过函数 access：$U\times D\rightarrow$ {True，False} 来定义。如果 role（u）= "requester" 且 level（u）$\geqslant$ level（d），则 access（u，d）= True，表示用户 u 有权限访问数据 d。管理操作通过函数 manage：$U\times D\times S\rightarrow S$ 来定义，表示管理员可以修改数据的安全级别。所有管理操作都会被记录到区块链上，通过函数 record：$(U\times D\times S)\cup(U\times D\times T)\rightarrow B$ 实现。

区块链网络主链 MC 通过验证后，分发给对应从链 SC，并执行交易 Tx，更新区块链状态，包括交易记录、

数据访问情况、读写下载操作等信息。区块链网络主链MC将已验证的交易 Tx 添加到区块中，并将该区块添加到区块链网络中。用户 U 和其他网络节点可以查询最新的区块链状态以验证交易执行。

2.3.3 主从多链用户科学数据共享流程

主从多链科学数据的共享是指在科研机构内部人员或其他科研机构用户之间，通过智能合约、IPFS 和混合加密机制实现了安全可靠的科学数据的共享，并使得用户在数据安全得到保障的前提下，激励数据提供者分享自己数据。即分为三个阶段，分别为系统初始化阶段、数据共享与存储阶段、产生激励奖励阶段，具体共享流程如图 3 所示。

（1）系统初始化阶段

主体人员科研工作者是 provider 角色 U 获取数据源后，科研工作者将现有数据、U 信息（地址信息、机构名称、职位等）、P 构成一个集合，dataMap = DataMap｛data，U ｛adress，orgName，rank｝，P｝。如果科研工作者是 requester 角色（即 P = Read | | Download）则忽略步骤（1），dataMap = DataMap ｛null，U ｛adress，orgName，rank｝，P｝。用私钥 SK_U 对请求进行签名，并把自己的公钥 PK_U，证书签名发送给 web app，web app 推送给 MC 进行验证：Sig_U = Sig（SK_U，dataMap），U - > web app - > MC:｛Sig_U，PK_U｝，如图 3 步骤（1）~（2）所示。

（2）数据共享与存储阶段

U 通过发送数据后，先调用 HARSC 验证 Sig_U 和 PK_U，判断 U 的身份信息、P（读、写、上传、下载）的权限、分级分类权限。如果验证不通过，则直接返回 ErrorMessage。如果验证通过，要判断 P 的权限，如果是写或上传操作则会上传至 IPFS，并返回 $Hash_{IPFS}$ 值存储于从链，如果是读或下载操作则会根据从链 $Hash_{IPFS}$ 查找对应 IPFS 数据，并返回交易情况。最后同步更新主链数据信息。如图 3 步骤（3）~（8）所示。

（3）产生激励奖励阶段

完成数据共享与存储阶段后，会在机构中积分池产生一定奖励给予数据提供者，根据用户身份获得对应奖励，同时会调用 DMSC，更新数据使用状态。最后返回结果，如果是分享数据则会返回 ture 或者 false，如果是获取数据则会返回数据。如图 3 步骤（9）~（12）所示。

3 实证分析

本文将对基于主从多链的科学数据保护与共享方法进行安全性能分析，并通过一系列实验来验证其有效性和效率，主要从存储开销、交易处理速度和交易次数三个方面对系统进行了实证研究。

3.1 安全性分析

（1）数据机密性

①加密：所有存储在区块链上的数据都进行了加密处理，即使数据被非法访问，没有对应的密钥也无法解读数据的实际内容。

②权限管理：本文通过 HARSC 来实现对数据访问权限的管理。只有在智能合约中被授权的地址才能访问对应的数据。

③安全通信：在节点之间的通信过程中，所有的数据传输都是通过安全的通道进行，防止了中间人攻击和数据泄露的风险。

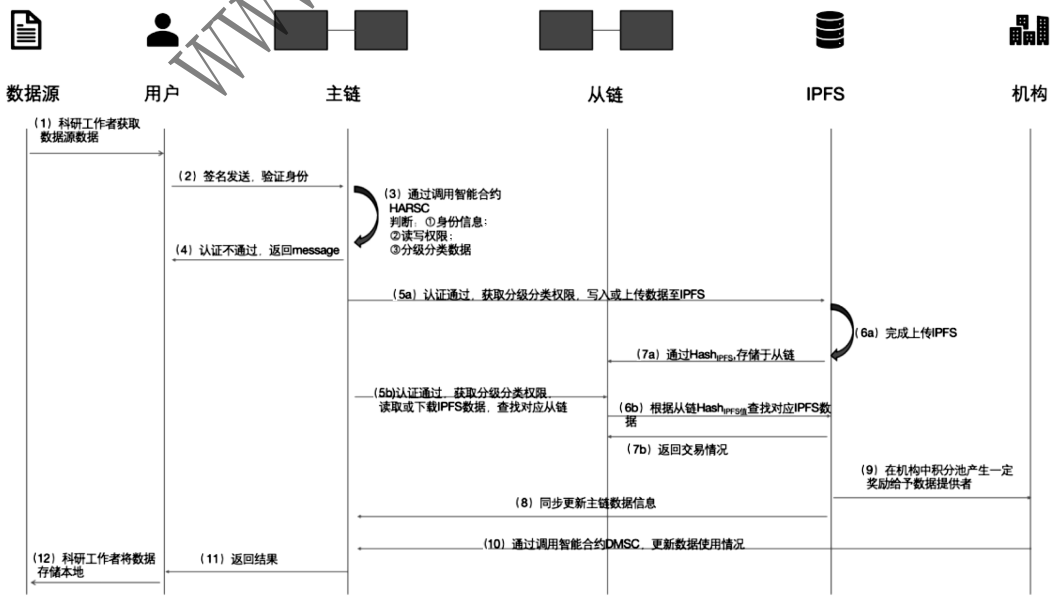

图 3 共享流程

（2）数据完整性

①区块链的不可篡改性：一旦数据被写入区块链，就无法被修改或删除。这保证了一旦数据被记录，其完整性就得到了保障。

②哈希校验：所有存储的数据都会被计算哈希值，并与数据一同存储。在数据检索时，通过重新计算数据的哈希值并与存储的哈希值进行对比，可以验证数据是否被篡改。

③共识机制：通过 ICNVSC，确保了不同节点上的数据是一致的，防止了因节点故障或恶意攻击导致的数据不一致问题。

（3）数据可用性

①分布式存储：通过将数据存储在分布式的节点上，即使部分节点发生故障，数据依然可以从其他节点上获取，保证了数据的高可用性。

②IPFS 的引入：通过引入 IPFS 作为数据存储层，进一步提升了数据的检索效率和可靠性，确保了数据的快速可用。

③负载均衡：在系统中采用了负载均衡机制，确保了在大量用户请求的情况下，系统依然能够保持稳定运行，提供持续的数据访问服务。

3.2 性能评估

为了全面评估基于主从多链的科学数据保护与共享方法的性能，实验的硬件环境为 3 台 Intel© Xeon© Bronze 3206R Processor CPU@ 3.60 GHz，64 GB RAM。实验环境为 PVE 中安装的 CentOS 7. 9，分配 4 GB 内存和两个核心处理器，虚拟化为 30 台服务器，实验所用计算机语言为 Go 语言。在不同的网络配置和负载条件下进行了一系列实验。

3.2.1 存储开销

实验结果显示，即使在节点数量较多的情况下，通过优化存储管理策略（如数据分级分类和数据分块），系统的存储开销仍然保持在一个可接受的范围内。对于每条从链，除了区块链本身的存储开销外，还有来自 IPFS 的额外存储开销。主链的存储开销 $S_m(t) = S_{m0} \times (1 + r_m)^t$，$S_{m0}$是主链的初始存储开销，$r_m$ 是主链存储开销的增长率。同理第 i 条从链的存储开销为 $S_{si}(t)$，第 i 条从链对接 IPFS 的存储开销 $S_{si}^{\mathrm{IPFS}}(t)$，总的存储开销 $S(t)$ 需要加上所有从链对接 IPFS 的存储开销：

$$S(t) = S_m(t) + \sum_{i=1}^{n} (S_{si}(t)) + S_{si}^{\mathrm{IPFS}}(t)) \tag{1}$$

实验表明，当到达一定时间，主从多链的存储开销明显优于是公共链（以太坊）。

优化后的存储开销图如图 4 所示。

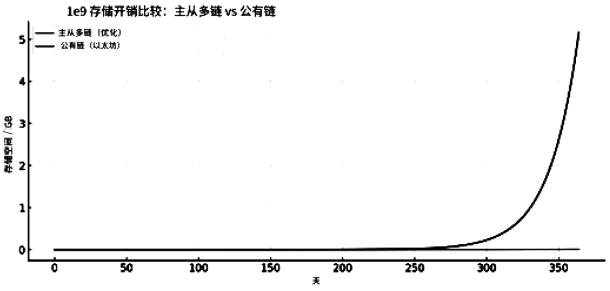

图 4　存储开销图

3.2.2 性能对比

经过优化的主从多链网络在性能上优于公链，能够满足大多数科学数据共享的需求。IPFS 存储可能会对系统的性能产生影响，特别是在数据检索时。可以为 IPFS 存储定义一个性能影响因子 ε（$0 \leqslant \varepsilon \leqslant 1$），其中 $\varepsilon = 0$ 表示没有性能影响，而 $\varepsilon = 1$ 表示性能降低到无法接受的程度。总的交易处理速度 $P(t)$ 需要减去由 IPFS 存储引起的性能损失：

$$P(t) = (P_m(t) + \sum_{i=1}^{n} P_{si}(t)) \times (1 - \varepsilon) \tag{2}$$

实验表明，随着时间的变化，每秒的交易量主从多链的方式是公共链（以太坊）的 3 倍。性能对比图如图 5 所示。

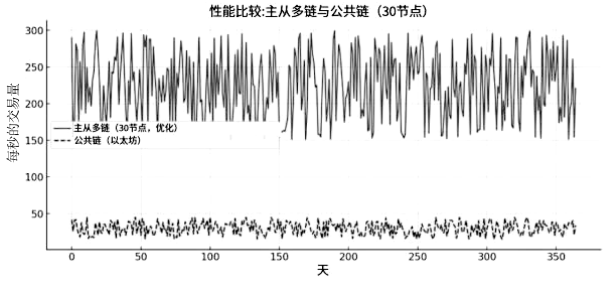

图 5　性能对比图

3.2.3 交易次数

本文评估了系统在处理大量交易时的稳定性和可靠性。实验结果表明，无论交易负载如何变化，系统都能够稳定运行，交易次数保持在一个较高的水平。总的交易次数 $T(t)$ 为：

$$T(t) = T_m(t) + \sum_{i=1}^{n} T_{si}(t) \tag{3}$$

交易次数图如图 6 所示。

通过比较实验数据，发现经过优化的主从多链网络在存储开销上有显著优势。主从多链网络在性能上优于单公链，并且接近公链和联盟链结合的性能。无论交易负载如何变化，主从多链网络都能够稳定处理大量交易，说明了系统的高稳定性和可靠性。

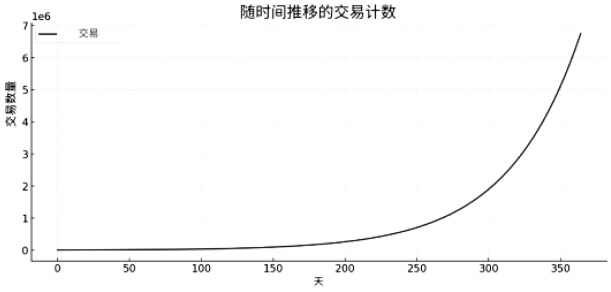

图 6　交易次数图

4　结论

在当前海量数据的大背景下，科学数据的分类与层级管理变得愈发重要，并呈现出明显的发展趋势。本文针对这一现象，提出了一种基于主从多链的科学数据保护与共享方法。以主从多链为思想，实现了角色访问控制、数据分级分类、科学数据智能合约（ICNVSC、HARSC、DMSC）的设计。实验证明，本研究在确保系统性能稳定的前提下，可保障多分类数据安全。但在实际应用中仍然存在一些问题和值得探讨的方向。首先，数据传输效率的问题还没有得到充分解决。链上与链下的互动过程常常会耗费大量的资源和时间，而 IPFS 在数据传输方面对带宽的需求也相对较高，这些因素都可能对系统的响应速度和用户体验造成影响。因此，未来的研究方向应当集中在优化存储模式和探索改进区块链共识算法上，以满足日益增长的数据处理需求。

参考文献

[1] 张雪媛，都平平，雷镭. 基于区块链技术的科学实验数据协同管理研究［J］. 情报杂志. 2022，41（8）：149－155.

[2] 胡剑，朱鹏，戚湧. 基于区块链的重大公共卫生事件下应急情报体系构建［J］. 情报理论与实践，2022，45（5）：156－164.

[3] 高洁. IPFS＋区块链技术在科学数据共享中的运用分析［J］. 图书情报导刊，2023，8（1）：35－39.

[4] AHMAD A，ASSD M，NJILLA L，et al. Blocktrail：a scalable multichain solution for blockchain-based audit trails［C］//Proceeding of the 2019 IEEE International Conference on Communications（ICC）. IEEE，2019：1－6.

[5] KAN L，WEI Y，MUHAMMAD A H，et al. A multiple blockchains architecture on inter-blockchain communication［C］//Proceeding of the 2018 IEEE International Conference on Software Quality，Reliability and Security Companion（QRS-C）. IEEE，2018：139－145.

[6] 刘扬，胡学先，周刚，等. 基于多层次区块链的医疗数据共享模型［J］. 计算机应用研究，2022，39（5）：1307－1312.

[7] 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.

[8] 李建霞，余丹丹. 科学数据共享平台用户感知有用性分析［J］. 情报杂志，2023，42（9）：196－201.

[9] 李涛. 基于区块链的主从多链及其共识算法研究［D］. 成都：电子科技大学，2022.

[10] CHOU I T，SU H H，HSUEH Y L，et al. BC-Store：a scalable design for blockchain storage［C］//Proceedings of the 2nd International Electronics Communication Conference. ACM，2020：33－38.

[11] 李莎莎，姬永清，罗盘，等. 针对主从多链的区块链集成共识机制研究［J］. 计算机技术与发展，2021，31（8）：82－86.

[12] 支凤稳，云仲伦，张闪闪. 基于区块链的个人科学数据共享模式研究［J］. 现代情报，2021，41（12）：69－78.

[13] 覃思航，代炜琦，曾海燕，等. 基于区块链的电力应用数据安全共享研究［J］. 信息网络安全，2023，23（8）：52－65.

[14] 盛小平，郭道胜. 科学数据开放共享中的数据安全治理研究［J］. 图书情报工作，2020，64（22）：25－36.

[15] 陈美宏，袁凌云，夏桐. 基于主从多链的数据分类分级访问控制模型［J］. 计算机应用，2024，44（4）：1148－1157.

[16] 都平平，李雨珂，张雪媛. 我国《科学数据管理办法》中概念视角数据域范畴与管理边界研究［J］. 图书馆杂志，2022，41（4）：96－105，114.

[17] RAKIB M H，HOSSAIN S，JAHAN M，et al. A Blockchain－Enabled Scalable Network Log Management System［J］. Joural of Computer Science，2022，18（6）：496－508.

（收稿日期：2024－08－19）

作者简介：

陈俊（1997－），男，硕士研究生，工程师，主要研究方向：数据安全、区块链、网络安全。

杨锐（1979－），通信作者，男，硕士研究生，高级工程师，主要研究方向：大数据挖掘分析技术、数据治理方法。E-mail：yangr@ mail. whlib. ac. cn。

李岚春（1987－），男，博士研究生，助理研究员，主要研究方向：科技情报、数据分析。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部